EBA/GL/2017/05

11/09/2017

Gairės

Gairės dėl IRT rizikos vertinimo per priežiūrinio tikrinimo ir vertinimo procesą (SREP)

1. Atitiktis gairėms ir informavimo pareiga

Šių gairių statusas

1. Šiame dokumente pateiktos pagal Reglamento (ES) Nr. 1093/20101 16 straipsnį parengtos gairės. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos ir finansų įstaigos turi dėti visas pastangas siekdamos laikytis šių gairių.

2. Gairėse išdėstoma EBI nuomonė dėl tinkamos priežiūros praktikos Europos finansų priežiūros institucijų sistemoje arba dėl to, kaip Sąjungos teisė turėtų būti taikoma tam tikroje srityje. Reglamento (ES) Nr. 1093/2010 4 straipsnio 2 dalyje apibrėžtos kompetentingos institucijos, kurioms taikomos šios gairės, turėtų jų laikytis ir atitinkamai jas įtraukti į savo praktiką (pvz., iš dalies pakeisti savo teisinę sistemą arba priežiūros procesus), įskaitant tuos atvejus, kai gairės pirmiausia yra skiriamos įstaigoms.

Pranešimo reikalavimai

3. Pagal Reglamento Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos iki 13.11.2017privalo EBI pranešti, ar laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Jeigu kompetentingos institucijos iki šio termino nepateiks jokio pranešimo, EBI laikys, kad jos gairių nesilaiko. Pranešimus reikėtų siųsti adresu compliance@eba.europa.eu užpildžius EBI interneto svetainėje pateiktą formą ir įrašius nuorodą „EBA/GL/2017/05“. Pranešimus turėtų teikti asmenys, turinys įgaliojimus pranešti apie gairių laikymąsi savo kompetentingų institucijų vardu. Apie visus gairių laikymosi pasikeitimus taip pat būtina pranešti EBI.

4. Pranešimai bus skelbiami EBI interneto svetainėje pagal 16 straipsnio 3 dalį.

[1] 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1093/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos bankininkystės institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/78/EB (OL L 331, 2010 12 15, p. 12).

2. Dalykas, taikymo sritis ir sąvokų apibrėžtys

Dalykas ir taikymo sritis

5. Šiomis pagal Direktyvos 2013/36/ES[2] 107 straipsnio 3 dalį parengtomis gairėmis siekiama užtikrinti priežiūros praktikos konvergenciją vertinant informacinių ir ryšių technologijų (IRT) riziką per priežiūrinio tikrinimo ir vertinimo procesą (SREP), nurodytą Direktyvos 2013/36/ES 97 straipsnyje ir išsamiau apibrėžtą EBI gairėse dėl bendros priežiūrinio tikrinimo ir vertinimo proceso (SREP) tvarkos ir metodikos[3]. Pirmiausia šiose gairėse konkrečiai nurodomi vertinimo kriterijai, kuriuos kompetentingos institucijos turėtų taikyti atlikdamos įstaigų valdymo, IRT strategijos vertinimą ir IRT rizikos pozicijų bei kontrolės priemonių priežiūrinį vertinimą. Šios gairės yra neatsiejama EBI SREP gairių dalis.

6. Kompetentingos institucijos šias gaires turėtų taikyti EBI SREP gairėse nurodytu SREP taikymo lygmeniu, laikydamosi jose nustatyto būtiniausio priežiūros intensyvumo modelio ir proporcingumo reikalavimų.

Kam gairės skirtos

7. Šios gairės skirtos Reglamento (ES) Nr. 1093/2010 4 straipsnio 2 dalies i punkte apibrėžtoms kompetentingoms institucijoms.

Sąvokų apibrėžtys

8. Jei nenurodyta kitaip, Direktyvoje 2013/36/ES, Reglamente (ES) Nr. 575/2013 vartojamos ir apibrėžtos sąvokos ir EBI SREP gairėse pateiktos apibrėžtys šiose gairėse vartojamos ta pačia reikšme. Be to, šiose gairėse vartojamos šios sąvokų apibrėžtys:

IRT sistemos	Informacinės ir ryšių technologijos, įdiegtos kaip mechanizmo arba tarpusavyje susijusio tinklo, kuriuo palaikomos įstaigos operacijos, dalis.

[2] 2013 m. birželio 26 d. Europos Parlamento ir Tarybos direktyva 2013/36/ES dėl galimybės verstis kredito įstaigų veikla ir dėl riziką ribojančios kredito įstaigų ir investicinių įmonių priežiūros, kuria iš dalies keičiama Direktyva 2002/87/EB ir panaikinamos direktyvos 2006/48/EB bei 2006/49/EB (1), OL L 176, 2013 6 27.

[3] EBA/GL/2014/13.

IRT paslaugos	IRT sistemomis vienam ar keliems vidaus arba išorės naudotojams teikiamos paslaugos. Prie jų priskiriamos, pvz., duomenų įvedimo, saugojimo, tvarkymo ir pranešimo paslaugos, taip pat stebėsenos, verslo paramos ir pagalbinės sprendimų priėmimo paslaugos.
IRT prieinamumo ir tęstinumo rizika	Neigiamo poveikio IRT sistemų ir duomenų veikimui ir jų prieinamumo rizika, įskaitant negalėjimą dėl IRT techninės arba programinės įrangos komponentų gedimo laiku atkurti įstaigos paslaugų; IRT sistemos valdymo trūkumus arba kitą įvykį, kaip išsamiau paaiškinta priede.
IRT saugumo rizika	Neteisėtos prieigos prie IRT sistemų ir duomenų iš įstaigos vidaus arba išorės rizika (pvz., kibernetiniai išpuoliai), kaip išsamiau paaiškinta priede.
IRT pakeitimų rizika	Rizika, kylanti dėl įstaigos negalėjimo laiku ir kontroliuotai valdyti IRT sistemos pakeitimų, pirmiausia susijusi su didelėmis ir sudėtingomis pakeitimų programomis, kaip išsamiau paaiškinta priede.
IRT duomenų vientisumo rizika	Rizika, kad IRT sistemose saugomi ir apdorojami duomenys gali būti neišsamūs, netikslūs arba nenuoseklūs įvairiose IRT sistemose, pvz., dėl silpnų arba netaikomų IRT kontrolės priemonių įvairiais IRT duomenų gyvavimo ciklo etapais (t. y. duomenų architektūros projektavimo, duomenų modelio ir (arba) duomenų žodynų kūrimo, įvesties duomenų patikros, duomenų išgavimo, perdavimo ir apdorojimo kontrolės, įskaitant perteiktus išvesties duomenis), dėl ko įstaiga tinkamai ir laiku gali nesuteikti paslaugų ir nepateikti (rizikos) valdymo ir finansinės informacijos, kaip išsamiau aprašyta priede.
IRT paslaugų pirkimo rizika	Rizika, kad pavedimas trečiajai šaliai arba kitam grupės subjektui (perkant paslaugas grupės viduje) teikti IRT sistemas arba susijusias paslaugas gali turėti neigiamą poveikį įstaigos veiklos rezultatams ir rizikos vertinimui, kaip išsamiau aprašyta priede.

3. Įgyvendinimas

Taikymo data

9. Šios gairės taikomos nuo 2018 m. sausio 1 d.

4. IRT rizikos vertinimo reikalavimai

1 antraštinė dalis. Bendrosios nuostatos

10. Atlikdamos SREP, kompetentingos institucijos turėtų įvertinti IRT riziką, valdymo sistemą ir IRT strategiją laikydamosi EBI SREP gairių 2 antraštinėje dalyje nurodyto būtiniausio priežiūros intensyvumo modelio ir proporcingumo kriterijų. Konkrečiai tai reiškia, kad:

    a. IRT rizikos vertinimo dažnumas turėtų priklausyti nuo būtiniausio priežiūros intensyvumo modelio, nustatyto pagal SREP kategoriją, prie kurios priskiriama įstaiga, ir konkrečios jos priežiūros analizės programos;

    b. IRT vertinimo išsamumas, detalumas ir intensyvumas turėtų būti proporcingas įstaigos dydžiui, struktūrai ir operacinei aplinkai, taip pat jos veiklos pobūdžiui, mastui ir sudėtingumui.

11. Proporcingumo principas šiose gairėse taikomas priežiūros veiklos mastui, dažnumui, intensyvumui, dialogo su įstaiga tvarkai ir su priežiūra susijusiems lūkesčiams dėl to, kokius standartus įstaiga turėtų atitikti.

12. Norėdamos atnaujinti vertinimą, kompetentingos institucijos gali remtis vertinant kitą riziką arba SREP elementus įstaigos arba kompetentingos institucijos jau atliktu darbu ir į jį atsižvelgti. Tiksliau, atlikdamos šiose gairėse nurodytus vertinimus, kompetentingos institucijos turėtų pasirinkti tinkamiausią priežiūrinio vertinimo metodą ir tokią metodiką, kuri geriausiai tinka ir yra proporcinga įstaigos atžvilgiu, ir savo įvertinimą turėtų grįsti esamais ir galimais gauti dokumentais (pvz., atitinkamomis ataskaitomis ir kitais dokumentais, susitikimų su (rizikos) vadovais informacija, per patikras vietoje nustatytais faktais).

13. Kompetentingos institucijos turėtų apibendrinti šiose gairėse nurodytų kriterijų vertinimų išvadas ir remtis jomis darydamos EBI SREP gairėse nurodyto SREP elementų vertinimo išvadas.

14. Tiksliau, atlikus valdymo ir IRT strategijos vertinimą pagal šių gairių 2 antraštinę dalį, turėtų būti padaromos išvados, kuriomis turėtų būti grindžiamas EBI SREP gairių 5 antraštinėje dalyje nurodyto SREP vidaus valdymo ir visos įstaigos kontrolės elemento vertinimo išvadų apibendrinimas ir į jas turėtų būti atsižvelgiama skiriant šiam SREP elementui atitinkamą balą. Be to, kompetentingos institucijos turėtų atsižvelgti į tai, kad į verslo modelio analizę pagal EBI SREP gairių 4 antraštinę dalį turėtų būti įtraukiamas visas reikšmingas neigiamas IRT strategijos vertinimo poveikis įstaigos verslo strategijai arba bet kokie rūpestį keliantys klausimai dėl to, kad įstaiga gali neturėti pakankamai IRT išteklių ir IRT pajėgumų svarbiems suplanuotiems strateginiams pakeitimams atlikti ir remti.

15. Šių gairių 3 antraštinėje dalyje nurodyto IRT rizikos vertinimo rezultatais turėtų būti grindžiamos operacinės rizikos vertinimo išvados ir turėtų būti laikoma, kad jais grindžiamas atitinkamas EBI SREP gairių 6.4 skirsnyje nurodytas balas.

16. Pažymėtina, kad paprastai kompetentingos institucijos rizikos pakategores turėtų įvertinti vertindamos pagrindines kategorijas (t. y. IRT rizika vertinama kaip operacinės rizikos dalis), bet kai kurias pakategores, kurias jos laiko reikšmingomis, jos gali vertinti atskirai. Šiuo tikslu, jei kompetentinga institucija nustato, kad IRT rizika yra reikšminga, šiose gairėse taip pat pateikiama balų lentelė (1 lentelė), kuri, taikant EBI SREP gairėse nurodytą bendrąjį kapitalui kylančios rizikos balo apskaičiavimo metodą, turėtų būti naudojama siekiant pateikti atskiros IRT rizikos pakategorės balą.

17. Spręsdamos, ar IRT rizika turėtų būti laikoma reikšminga, kad ją būtų galima įvertinti balais kaip atskirą operacinės rizikos pakategorę, kompetentingos institucijos gali taikyti EBI SREP gairių 6.1 skirsnyje nurodytus kriterijus.

18. Taikydamos šias gaires kompetentingos institucijos prireikus turėtų atsižvelgti į priede pateiktą neišsamų IRT rizikos pakategorių ir rizikos scenarijų sąrašą, pažymint, kad šiame priede daugiausia dėmesio skiriama tokiai IRT rizikai, dėl kurios gali atsirasti didelio masto nuostolių. Kompetentingos institucijos gali neįtraukti kai kurios į klasifikaciją įtrauktos su jų vertinimu nesusijusios IRT rizikos. Įstaigos turėtų ne taikyti priede pateiktą IRT klasifikaciją, bet prižiūrėti savo pačių rizikos klasifikaciją.

19. Kai šios gairės taikomos tarpvalstybinėms bankų grupėms ir jų subjektams ir yra įkurta priežiūros institucijų kolegija, atitinkamos kompetentingos institucijos, bendradarbiaudamos per SREP vertinimą pagal EBI SREP gairių 11.1 skirsnį, kiek galėdamos suderina tiksliai ir išsamiai apibrėžtą kiekvieną informacijos straipsnį, ir šiuos reikalavimus nuosekliai taiko visiems grupės subjektams.

2 antraštinė dalis. Įstaigų valdymo ir IRT strategijos vertinimas

2.1 Bendrieji principai

20. Kompetentingos institucijos turėtų vertinti, ar įstaigos bendroji valdymo ir vidaus kontrolės sistema tinkamai taikoma IRT sistemoms ir susijusiai rizikai ir ar valdymo organas tinkamai atsižvelgia į šiuos aspektus ir juos valdo, nes IRT yra neatsiejamos nuo tinkamo įstaigos veikimo.

21. Atlikdamos šį vertinimą, kompetentingos institucijos turėtų laikytis EBI vidaus valdymo gairėse (GL 44)[4] ir tarptautinėse šios srities gairėse nurodytų gero vidaus valdymo ir rizikos kontrolės organizavimo reikalavimų ir standartų tiek, kiek jie taikomi atsižvelgiant į IRT sistemų ir rizikos specifiką.

22. Šioje antraštinėje dalyje nurodytas vertinimas neapima specifinių IRT sistemos valdymo, rizikos valdymo ir kontrolės priemonių elementų, kuriais pirmiausia siekiama valdyti specifinę IRT riziką, nurodytą šių gairių 3 antraštinėje dalyje, bet pirmiausia atsižvelgiama į šias sritis:

    a. IRT strategiją – ar įstaiga taiko tinkamai valdomą ir su jos verslo strategija derančią IRT strategiją;

    b. bendrąjį vidaus valdymą – ar įstaigos bendrojo vidaus valdymo sistema yra tinkama įstaigos IRT sistemoms;

    c. IRT riziką įstaigos rizikos valdymo sistemoje – ar įstaigos rizikos valdymo ir vidaus kontrolės sistema tinkamai apsaugomos įstaigos IRT sistemos.

23. Teikiant informaciją apie įstaigos valdymo elementus, 22 punkto a papunkčio informacija pirmiausia turėtų būti grindžiamas EBI SREP gairių 4 antraštinėje dalyje aprašytas verslo modelio vertinimas. b ir c punktai turėtų išsamiau papildyti vertinimus EBI SREP gairių 5 antraštinėje dalyje aprašytais klausimais, o šiose gairėse aprašyto vertinimo duomenys turėtų būti naudojami atliekant atitinkamą vertinimą pagal EBI SREP gairių 5 antraštinę dalį.

24. Šio vertinimo rezultatais prireikus turėtų būti remiamasi vertinant rizikos valdymą ir kontrolės priemones pagal šių gairių 3 antraštinę dalį.

2.2 IRT strategija

25. Pagal šį skirsnį kompetentingos institucijos turėtų įvertinti, ar įstaiga taiko IRT strategiją, kurią tinkamai prižiūri įstaigos valdymo organas; kuri dera su verslo strategija, pirmiausia siekiant išsaugoti savo IRT aktualumą ir planuoti arba įgyvendinti svarbius ir sudėtingus IRT pakeitimus; ir kuria remiamas įstaigos verslo modelis.

[4] EBI vidaus valdymo gairės, GL 44, 2011 m. rugsėjo 27 d.

2.2.1 IRT strategijos rengimas ir tinkamumas

26. Kompetentingos institucijos turėtų vertinti, ar įstaiga taiko jos IRT veiklos pobūdžiui, mastui ir sudėtingumui proporcingą įstaigos IRT strategijos rengimo ir tobulinimo sistemą. Atlikdamos šį vertinimą, kompetentingos institucijos turėtų atsižvelgti į tai, ar:

    a. verslo linijos (-ų) vyresnioji vadovybė[5] tinkamai dalyvauja apibrėžiant įstaigos strateginius IRT prioritetus ir ar IRT funkcijos vyresnioji vadovybė yra informuota apie pagrindinių verslo strategijų ir iniciatyvų rengimą, projektavimą ir inicijavimą siekiant užtikrinti nuolatinį IRT sistemų, IRT paslaugų ir IRT funkcijos (t. y. už šių sistemų ir paslaugų valdymą ir naudojimąsi jomis atsakingų asmenų) ir įstaigos verslo strategijos derėjimą tarpusavyje ir ar IRT veiksmingai naujinamos;

    b. IRT strategija dokumentuojama ir papildoma konkrečiais įgyvendinimo planais, pirmiausia susijusiais su svarbiais orientyrais ir išteklių planavimu (įskaitant finansinius ir žmogiškuosius išteklius), siekiant užtikrinti, kad jie būtų tikroviški ir pagal juos būtų galima įgyvendinti IRT strategiją;

    c. įstaiga periodiškai naujina IRT strategiją, ypač jei keičia verslo strategiją, siekdama užtikrinti nuolatinį IRT ir vidutinės trukmės bei ilgalaikių verslo tikslų, planų ir veiklos derėjimą;

    d. įstaigos valdymo organas patvirtina IRT strategiją, jos įgyvendinimo planus ir stebi jos įgyvendinimą.

2.2.2 IRT strategijos įgyvendinimas

27. Jei pagal įstaigos IRT strategiją reikia įgyvendinti svarbius ir sudėtingus IRT pakeitimus arba pakeitimus, darančius reikšmingą poveikį įstaigos verslo modeliui, kompetentingos institucijos turėtų įvertinti, ar įstaiga taiko kontrolės sistemą, tinkamą jos dydžiui, su IRT susijusiai veiklai ir pakeitimų veiklos lygmeniui, kuria remiamas veiksmingas įstaigos IRT strategijos įgyvendinimas. Atlikdamos šį vertinimą, kompetentingos institucijos turėtų atsižvelgti į tai, ar ši kontrolės sistema atitinka šiuos reikalavimus:

    a. į ją įtraukti valdymo procesai (pvz., pažangos ir biudžeto stebėsena ir ataskaitų teikimas) ir atitinkami organai (pvz., projektų valdymo biuras, IRT valdančioji grupė arba lygiavertis organas), kad būtų galima veiksmingai remti IRT strateginių programų įgyvendinimą;

    b. joje apibrėžtos ir paskirtos IRT strateginių programų įgyvendinimo pareigos ir atsakomybė, ypatingą dėmesį skiriant pagrindinių suinteresuotųjų subjektų, dalyvaujančių organizuojant, valdant ir stebint svarbius ir sudėtingus IRT pakeitimus, patirčiai ir platesnio poveikio organizacijai ir žmogiškiesiems ištekliams valdymui (pvz., nenorėjimo keistis, mokymo, komunikacijos valdymui);

    c. ją įgyvendinant dalyvauja nepriklausomi kontrolės ir vidaus audito funkcijų vykdytojai, teikiantys patikinimą, kad su IRT strategijos įgyvendinimu susijusi rizika buvo nustatyta,

[5] Vyresnioji vadovybė ir valdymo organas apibrėžti 2013 m. birželio 26 d. Direktyvos 2013/36/ES 3 straipsnio 7 punkte „valdymo organas“ ir 9 punkte „vyresnioji vadovybė“.

įvertinta ir veiksmingai sumažinta ir kad taikoma IRT strategijos valdymo sistema yra veiksminga;

d. į ją įtrauktas planavimo ir jo peržiūros procesas, kurį taikant galima lanksčiai atsižvelgti į svarbius nustatytus klausimus (pvz., patirtas įgyvendinimo problemas arba vėlavimą) arba išorės pokyčius (pvz., svarbius verslo aplinkos pokyčius, su technologijomis susijusius klausimus arba inovacijas), kad būtų užtikrinta, jog bus laiku pritaikomas strateginis įgyvendinimo planas.

2.3 Bendrasis vidaus valdymas

28. Pagal EBI SREP gairių 5 antraštinę dalį kompetentingos institucijos turėtų vertinti, ar įstaigos organizacinė struktūra yra tinkama, skaidri ir tinka „pagal paskirtį“ ir ar įstaiga yra tinkamai organizavusi vidaus valdymą. Konkrečiai kalbant apie IRT sistemas ir atsižvelgiant į EBI vidaus valdymo gaires, atliekant šį vertinimą reikėtų vertinti bent tai, ar įstaigoje aiškiai matyti:

a) patikima ir skaidri organizacinė struktūra, kurioje aiškiai paskirstytos IRT atsakomybės sritys, įskaitant valdymo organą ir jo komitetus, ir kad pagrindiniai už IRT atsakingi asmenys (pvz., vyriausiasis informacijos pareigūnas, vyriausiasis už veiklą atsakingas pareigūnas arba panašias pareigas einantis asmuo) gali tinkamai netiesiogiai arba tiesiogiai susisiekti su valdymo organu, siekiant užtikrinti, kad svarbi su IRT susijusi informacija arba klausimai būtų tinkamai pranešami, aptariami ir sprendimai dėl jų būtų priimami valdymo organo lygmeniu;

b) valdymo organas išmano su IRT susijusią riziką ir ją mažina.

29. Pagal EBI SREP gairių 5.2 skirsnį kompetentingos institucijos turėtų vertinti, ar įstaigos vykdoma IRT paslaugų pirkimo politika ir strategija prireikus atsižvelgiama į IRT paslaugų pirkimo poveikį įstaigos veiklai ir verslo modeliui.

2.4 IRT rizika įstaigos rizikos valdymo sistemoje

30. Vertindamos visos įstaigos rizikos valdymą ir vidaus kontrolės priemones, kaip nurodyta EBI SREP gairių 5 antraštinėje dalyje, kompetentingos institucijos turėtų atsižvelgti į tai, ar, taikant įstaigos rizikos valdymo ir vidaus kontrolės sistemą, suteikiama tinkama įstaigos IRT sistemų apsauga, atitinkanti įstaigos dydį, veiklą ir IRT rizikos profilį, kaip apibrėžta 3 antraštinėje dalyje. Pirmiausia kompetentingos institucijos turėtų nustatyti, ar:

a. apibrėžiant bendrąją rizikos strategiją ir nustatant vidaus kapitalą, į norimą prisiimti riziką ir ICAAP įtraukta prie platesnės operacinės rizikos kategorijos priskiriama IRT rizika;

b. IRT rizika įtraukta į visos įstaigos rizikos valdymo ir vidaus kontrolės sistemų taikymo sritį.

31. Kompetentingos institucijos turėtų atlikti a papunktyje nurodytą vertinimą, atsižvelgdamos į tikėtinus ir nepalankius scenarijus, pvz., scenarijus, įtrauktus į pagal konkrečią įstaigą pritaikytą arba priežiūrinį testavimą nepalankiausiomis sąlygomis.

32. Konkrečiai dėl b papunkčio kompetentingos institucijos turėtų vertinti, ar EBI gairių 104 punkto a ir d papunkčiuose bei 105 punkto a ir c papunkčiuose aprašytos nepriklausomos kontrolės ir vidaus audito funkcijos, atsižvelgiant į įstaigos dydį ir IRT rizikos profilį, yra tinkamos pakankamam IRT ir kontrolės bei audito funkcijų nepriklausomumui užtikrinti.

2.5 Išvadų apibendrinimas

33. Šie rezultatai turėtų būti išdėstomi EBI SREP gairių 5 antraštinėje dalyje nurodytoje išvadų santraukoje ir įtraukiami į atitinkamą balą, nustatytą remiantis EBI SREP gairių 3 lentelėje nurodytais analizės kriterijais.

34. Siekiant padaryti pirmiau nurodyto vertinimo išvadas, vertinant IRT strategiją turėtų būti atsižvelgiama į šiuos aspektus:

    a. jei kompetentingos institucijos prieina prie išvados, kad įstaigos valdymo sistema yra netinkama įstaigos IRT strategijai pagal 2.2 skirsnį rengti ir įgyvendinti, šia išvada turėtų būti remiamasi atliekant EBI SREP gairių 5 antraštinės dalies 87 punkto a papunktyje nurodytą įstaigos vidaus valdymo vertinimą;

    b. jei kompetentingos institucijos, atlikusios pirmiau 2.2 skirsnyje nurodytus vertinimus, prieina prie išvados, kad IRT strategija ir verslo strategija yra visiškai nesuderintos ir kad tai galėtų daryti reikšmingą neigiamą poveikį įstaigos ilgalaikiams veiklos ir (arba) finansiniams tikslams, įstaigos tvarumui ir (arba) verslo modeliui arba įstaigos verslo sritims ir (arba) linijoms, kurios pagal EBI SREP gairių 62 punkto a papunktį nustatytos kaip reikšmingiausios, šia išvada turėtų būti remiamasi atliekant SREP gairių 4 antraštinės dalies 70 punkto b ir c papunkčiuose nurodytą verslo modelio vertinimą;

    c. jei kompetentingos institucijos, atlikusios pirmiau 2.2 skirsnyje nurodytus vertinimus, prieina prie išvados, kad įstaiga gali neturėti pakankamai IRT išteklių ir IRT įgyvendinimo pajėgumų svarbiems suplanuotiems strateginiams pakeitimams atlikti ir remti, šia išvada turėtų būti remiamasi atliekant EBI SREP gairių 4 antraštinės dalies 70 punkto b papunktyje nurodytą verslo modelio vertinimą.

3 antraštinė dalis. Įstaigos IRT rizikos pozicijų ir kontrolės priemonių vertinimas

3.1 Bendrosios nuostatos

35. Kompetentingos institucijos turėtų vertinti, ar įstaiga yra tinkamai nustačiusi, įvertinusi ir sumažinusi jai kylančią IRT riziką. Šis procesas turėtų būti įtrauktas į operacinės rizikos valdymo sistemą ir derėti su operacinei rizikai taikomu metodu.

36. Iš pradžių kompetentingos institucijos turėtų nustatyti reikšmingą būdingą įstaigai kylančią arba galinčią kilti IRT riziką, o paskui įvertinti įstaigos IRT rizikos valdymo sistemos, procedūrų ir kontrolės priemonių, kuriomis ši rizika mažinama, veiksmingumą. Vertinimo rezultatai turėtų būti išdėstomi išvadų santraukoje, kuria grindžiamas SREP gairėse nurodytas operacinės rizikos balas. Jei IRT rizika laikoma reikšminga ir kompetentingos institucijos nori skirti jai atskirą balą, smulkesnės operacinės rizikos balas turėtų būti skiriamas naudojantis 1 lentele.

37. Atlikdamos vertinimą pagal šią antraštinę dalį, kompetentingos institucijos, siekdamos nustatyti įstaigos priežiūrinio vertinimo prioritetus, turėtų remtis visais esamais EBI SREP gairių 6 antraštinės dalies 127 punkte nurodytais informacijos šaltiniais, pvz., įstaigos rizikos valdymo veikla, ataskaitomis ir rezultatais. Atlikdamos šį vertinimą kompetentingos institucijos taip pat turėtų naudotis kitais informacijos šaltiniais, įskaitant, jei taikoma:

    a. įstaigos atliktus savo IRT rizikos ir kontrolės priemonių vertinimus (jei jie pateikti ICAAP informacijoje);
    b. įstaigos valdymo organui pateiktą su IRT rizika susijusią valdymo informaciją, pvz., periodines ir dėl incidentų pateiktas IRT rizikos ataskaitas (įskaitant įtrauktąsias į veiklos nuostolių duomenų bazę), iš įstaigos rizikos valdymo funkcijos vykdytojų gautus IRT rizikos duomenis;
    c. įstaigos audito komitetui praneštus nustatytus IRT vidaus ir išorės auditų faktus.

3.2 Reikšmingos IRT rizikos nustatymas

38. Imdamosi toliau nurodytų veiksmų, kompetentingos institucijos turėtų nustatyti reikšmingą įstaigai kylančią arba galinčią kilti IRT riziką.

3.2.1 Įstaigos IRT rizikos profilio patikra

39. Tikrindamos įstaigos IRT rizikos profilį, kompetentingos institucijos turėtų atsižvelgti į visą svarbią informaciją apie įstaigos IRT rizikos pozicijas, įskaitant 37 punkte nurodytą informaciją, taip pat į nustatytus reikšmingus šių gairių 2 antraštinėje dalyje nurodytos IRT organizacijos ir visos įstaigos kontrolės priemonių trūkumus arba silpnuosius aspektus ir, jei taikoma, proporcingai patikrinti šią informaciją. Atlikdamos šią patikrą, kompetentingos institucijos turėtų atsižvelgti į:

a. galimą reikšmingo įstaigos IRT sistemų sutrikimo poveikį šalies arba tarptautinio lygmens finansų sistemai;
b. tai, ar įstaigai gali kilti IRT saugumo rizika arba IRT prieinamumo ir tęstinumo rizika dėl priklausomumo nuo interneto, įdiegtų gausių novatoriškų IRT sprendimų arba kitų verslo platinimo kanalų, dėl kurių labiau tikėtina, kad ji gali tapti kibernetinių išpuolių taikiniu;
c. tai, ar įstaigai gali kilti didesnė IRT saugumo rizika, IRT prieinamumo ir tęstinumo rizika, IRT duomenų vientisumo rizika arba IRT pakeitimų rizika dėl jos IRT sistemų sudėtingumo (pvz., dėl susiliejimo arba įsigijimų) arba senumo;
d. tai, ar įstaiga įgyvendina reikšmingus savo IRT sistemų ir (arba) IRT funkcijos pakeitimus (pvz., dėl susiliejimo, įsigijimų, investicijų pardavimo arba pagrindinių IRT sistemų pakeitimo), galinčių turėti neigiamą poveikį IRT sistemų stabilumui arba tinkamam veikimui ir kelti reikšmingą IRT prieinamumo ir tęstinumo riziką, IRT saugumo riziką, IRT pakeitimų riziką arba IRT duomenų vientisumo riziką;
e. tai, ar įstaiga perka IRT paslaugas arba IRT sistemas iš grupės arba ne grupės subjektų ir dėl to jai gali kilti reikšminga IRT paslaugų pirkimo rizika;
f. tai, ar įstaiga įgyvendina drastiškas IRT sąnaudų mažinimo priemones, dėl kurių gali sumažėti reikiamos IRT investicijos, ištekliai, IT praktinė patirtis ir padidėti visų rūšių į klasifikaciją įtraukta IRT rizika;
g. tai, ar svarbios IRT veiklos ir (arba) duomenų centrų vietovėse (pvz., regionuose, šalyse) įstaigai kyla pavojus dėl gaivalinių nelaimių (pvz., potvynių, žemės drebėjimų), politinio nestabilumo arba darbo konfliktų ir pilietinių neramumų, dėl kurių gali reikšmingai padidėti IRT prieinamumo ir tęstinumo rizika ir IRT saugumo rizika.

3.2.2 Ypatingos svarbos IRT sistemų ir paslaugų patikra

40. Siekdamos nustatyti IRT riziką, galinčią turėti įstaigai prudencinį poveikį, kompetentingos institucijos turėtų patikrinti įstaigos dokumentus ir susidaryti nuomonę dėl to, kurios IRT sistemos ir paslaugos yra itin svarbios tinkamam su esmine įstaigos veikla susijusiam veikimui, prieinamumui, tęstinumui ir saugumui.

41. Šiuo tikslu kompetentingos institucijos turėtų tikrinti įstaigos taikomą ypatingos svarbos IRT sistemų ir paslaugų nustatymo metodiką ir procesus, atsižvelgdamos į tai, kad kai kurias IRT sistemas ir paslaugas įstaiga gali laikyti ypatingos svarbos dėl veiklos tęstinumo ir prieinamumo, saugumo (pvz., sukčiavimo prevencijos) ir (arba) konfidencialumo (pvz., konfidencialių duomenų). Atlikdamos šią patikrą, kompetentingos institucijos turėtų atsižvelgti į tai, kad ypatingos svarbos IRT sistemos ir paslaugos turėtų atitikti bent vieną iš šių sąlygų:

a. jomis palaikomos įstaigos esminės veiklos operacijos ir platinimo kanalai (pvz., bankomatai, internetinė ir mobilioji bankininkystė);
b. jomis palaikomi esminiai valdymo procesai ir organizacinės funkcijos, įskaitant rizikos valdymą (pvz., rizikos valdymo ir iždo valdymo sistemos);
c. joms taikomi specialūs teisiniai arba reguliavimo reikalavimai (jei tokių reikalavimų yra), kuriais kai kurioms sisteminės svarbos paslaugoms nustatomi (jei taikoma) griežtesni prieinamumo, atsparumo, konfidencialumo arba saugumo reikalavimai (pvz., duomenų apsaugos teisės aktai

arba galimi RTO (angl. *Recovery Time Objectives* – ilgiausias laikotarpis, per kurį po incidento sistemą arba procesą būtina atkurti) ir RPO (angl. *Recovery Point Objective* – ilgiausias laikotarpis, per kurį, įvykus incidentui, gali būti prarasti duomenys) tikslai;

d. jomis apdorojami ir jose saugomi konfidencialūs arba neskelbtini duomenys, su kuriais susijusi neteisėta prieiga galėtų turėti reikšmingos įtakos įstaigos reputacijai, finansiniams rezultatams arba veiklos patikimumui ir tęstinumui (pvz., duomenų bazėms, kuriose saugomi neskelbtini klientų duomenys); ir (arba)

e. jomis teikiamos pagrindinės funkcijos, gyvybiškai svarbios, kad įstaiga galėtų tinkamai veikti (pvz., telekomunikacijų ir ryšių paslaugos, IRT ir kibernetinio saugumo paslaugos).

3.2.3 Ypatingos svarbos IRT sistemoms ir paslaugoms kylančios reikšmingos IRT rizikos nustatymas

42. Atsižvelgdamos į pirmiau nurodytas įstaigos IRT rizikos profilio ir ypatingos svarbos IRT sistemų ir paslaugų patikras, kompetentingos institucijos turėtų susidaryti nuomonę dėl reikšmingos IRT rizikos, kuri, remiantis priežiūrinėmis išvadomis, gali turėti reikšmingą prudencinį poveikį įstaigos ypatingos svarbos IRT sistemoms ir paslaugoms.

43. Vertindamos galimą IRT rizikos poveikį įstaigos ypatingos svarbos IRT sistemoms ir paslaugoms, kompetentingos institucijos turėtų atsižvelgti į:

a. finansinį poveikį, įskaitant (bet ne tik) lėšų arba turto praradimą, galimą atlyginimą klientams, teisines ir ištaisymo išlaidas, sutartinę žalą, prarastas pajamas;

b. galimą veiklos sutrikimą, atsižvelgiant (be kita ko) į susijusių finansinių paslaugų svarbą; galimai susijusių klientų ir (arba) filialų ir darbuotojų skaičių;

c. galimą poveikį įstaigos reputacijai, remiantis susijusios bankininkystės paslaugos arba operacinės veiklos svarba (pvz., klientų duomenų vagystė); susijusių IRT sistemų ir paslaugų išoriniu profiliu ir (arba) matomumu (pvz., mobiliosios arba internetinės bankininkystės sistemos, pardavimo vieta, bankomatas arba mokėjimo sistemos);

d. reguliavimo poveikį, įskaitant viešai pareikštą reguliavimo institucijų nepasitikėjimą, baudas arba net leidimų keitimą.

e. strateginį poveikį įstaigai, pvz., jei pakenkiama strateginiams produktams ar verslo planams arba jei šie produktai ar planai pavagiami.

44. Paskui kompetentingos institucijos reikšminga laikomą nustatytą IRT riziką turėtų priskirti prie toliau nurodytų IRT rizikos kategorijų; į jas patenkanti rizika papildomai aprašyta ir jos pavyzdžių pateikta priede. Atlikdamos 3 antraštinėje dalyje nurodytą vertinimą, kompetentingos institucijos turėtų atsižvelgti į priede nurodytą IRT riziką:

a. IRT prieinamumo ir tęstinumo riziką,
b. IRT saugumo riziką,
c. IRT pakeitimų riziką,

d. IRT duomenų vientisumo riziką,
e. IRT paslaugų pirkimo riziką.

Priskiriant šią riziką, kompetentingoms institucijoms turėtų būti lengviau nustatyti, kuri rizika yra reikšminga (jei tokios rizikos yra), ir todėl turėtų būti atliekamas atidesnis ir (arba) išsamesnis tikrinimas atliekant toliau nurodytus vertinimo veiksmus.

3.3 Kontrolės priemonių, kuriomis mažinama reikšminga IRT rizika, vertinimas

45. Siekdamos įvertinti įstaigos likutinės IRT rizikos poziciją, kompetentingos institucijos turėtų tikrinti, kaip įstaiga nustato, stebi, vertina ir mažina reikšmingą riziką, kurią kompetentingos institucijos nustatė atlikdamos pirmiau nurodytą vertinimą.

46. Šiuo tikslu dėl nustatytos reikšmingos IRT rizikos kompetentingos institucijos turėtų tikrinti, jei taikoma:

a. IRT rizikos valdymo politiką, procesus ir priimtinos rizikos ribines vertes;
b. organizacijos valdymo ir priežiūros sistemą;
c. vidaus audito apimtį ir nustatytus faktus;
d. nustatytai reikšmingai IRT rizikai taikomas specialias IRT rizikos kontrolės priemones.

47. Atliekant šį vertinimą turėtų būti atsižvelgiama į EBI SREP gairių 5 antraštinėje dalyje nurodytos bendrosios rizikos valdymo ir vidaus kontrolės sistemos analizės rezultatus, taip pat į šių gairių 2 antraštinėje dalyje nurodytą įstaigos valdymą ir strategiją, nes nustatyti reikšmingi šių sričių trūkumai gali turėti įtakos įstaigos gebėjimui valdyti ir mažinti jai kylančią IRT riziką. Prireikus kompetentingos institucijos taip pat turėtų naudotis šių gairių 37 punkte nurodytais informacijos šaltiniais.

48. Toliau nurodytus vertinimo veiksmus kompetentingos institucijos turėtų atlikti taip, kad jie būtų proporcingi įstaigos veiklos pobūdžiui, mastui ir sudėtingumui, ir atlikti įstaigos IRT rizikos profiliui tinkamą priežiūrinį tikrinimą.

3.3.1 IRT rizikos valdymo politika, procesai ir priimtinos rizikos ribinės vertės

49. Kompetentingos institucijos turėtų tikrinti, ar nustatytai reikšmingai IRT rizikai įstaiga taiko tinkamą rizikos valdymo politiką, procesus ir priimtinos rizikos ribines vertes. Jie gali būti įtraukti į operacinės rizikos valdymo sistemą arba išdėstyti atskirame dokumente. Atlikdamos šį vertinimą, kompetentingos institucijos turėtų atsižvelgti į tai, ar:

a. rizikos valdymo politika tinkamai įforminta, ją yra patvirtinęs valdymo organas ir joje pateikta pakankamai gairių dėl įstaigos norimos prisiimti IRT rizikos ir pagrindinių siekiamų IRT rizikos valdymo tikslų ir (arba) taikomų priimtinos IRT rizikos ribinių verčių. Apie atitinkamą IRT rizikos valdymo politiką taip pat turėtų būti pranešama visiems susijusiems suinteresuotiesiems subjektams;

b. taikoma politika apima visus reikšmingus nustatytos reikšmingos IRT rizikos valdymo elementus;

c. įstaiga yra įgyvendinusi susijusios reikšmingos IRT rizikos nustatymo (pvz., įstaigos atliekamo savo rizikos kontrolės vertinimo, rizikos scenarijų analizės) ir stebėsenos procesą bei susijusias procedūras;

d. įstaiga taiko IRT rizikos valdymo ataskaitų teikimo sistemą, pagal kurią vyresniajai vadovybei ir valdymo organui laiku teikiama informacija ir pagal kurią vyresnioji vadovybė ir (arba) valdymo organas gali įvertinti ir stebėti, ar įstaigos IRT rizikos mažinimo planai ir priemonės dera su patvirtinta norima prisiimti rizika ir (arba) priimtinos rizikos ribinėmis vertėmis (jei taikoma), taip pat stebėti reikšmingos IRT rizikos pokyčius.

3.3.2 Organizacijos valdymo ir priežiūros sistema

50. Kompetentingos institucijos turėtų vertinti, kaip taikomos rizikos valdymo pareigos ir atsakomybė įtrauktos ir integruotos į vidaus organizaciją, siekiant valdyti ir prižiūrėti nustatytą reikšmingą IRT riziką. Šiuo atžvilgiu kompetentingos institucijos turėtų vertinti, ar įstaigoje aiškiai matyti, kad:

a. nustatytos aiškios pareigos ir atsakomybė už susijusios reikšmingos IRT rizikos nustatymą, vertinimą, stebėseną, mažinimą, pranešimą apie ją ir jos priežiūrą;

b. apie su rizika susijusią atsakomybę ir pareigas aiškiai informuojama, jos paskiriamos ir įtraukiamos į visas susijusias dalis (pvz., verslo linijas, IT) ir organizacijos procesus, įskaitant pareigas ir atsakomybę už rizikos informacijos rinkimą, apibendrinimą ir pranešimą vyresniajai vadovybei ir (arba) valdymo organui;

c. IRT rizikos valdymo veikla vykdoma naudojantis pakankamais ir tinkamos kokybės žmogiškaisiais ir techniniais ištekliais. Siekdamos įvertinti taikomų rizikos mažinimo planų patikimumą, kompetentingos institucijos taip pat turėtų vertinti, ar įstaiga yra skyrusi pakankamą finansinį biudžetą ir (arba) pakankamai kitų reikiamų šių planų įgyvendinimo išteklių;

d. valdymo organas imasi tinkamų tolesnių veiksmų ir atsakomųjų priemonių dėl svarbių nepriklausomų kontrolės funkcijų vykdytojų nustatytų faktų apie IRT riziką, atsižvelgiant į galimą pavedimą kai kuriuos aspektus nagrinėti komitetui, jei toks komitetas įsteigtas;

e. taikomų IRT taisyklių ir politikos taikymo išimtys yra užregistruotos ir kad nepriklausomi kontrolės funkcijos vykdytojai atlieka dokumentuotą jų patikrą ir teikia ataskaitas, ypatingą dėmesį atkreipdami į susijusią riziką.

3.3.3 Vidaus audito apimtis ir nustatyti faktai

51. Kompetentingos institucijos turėtų atsižvelgti į tai, ar vidaus audito funkcijos vykdytojai veiksmingai audituoja taikomą IRT rizikos kontrolės sistemą, ir šiuo tikslu tikrinti, ar:

a. IRT rizikos kontrolės sistemos auditas atliekamas pakankamai kokybiškai, išsamiai, dažnai ir atitinka įstaigos dydį, veiklą ir IRT rizikos profilį;

b. į audito planą įtraukti įstaigos nustatytos ypatingos svarbos IRT rizikos auditai;

c. svarbūs nustatyti IRT audito faktai, įskaitant sutartus veiksmus, pranešami valdymo organui;

d. dėl nustatytų IRT audito faktų, įskaitant sutartus veiksmus, imamasi tolesnių veiksmų, o vyresnioji vadovybė ir (arba) audito komitetas periodiškai tikrina pažangos ataskaitas.

3.3.4 Nustatytai reikšmingai IRT rizikai taikomos specialios IRT rizikos kontrolės priemonės

52. Dėl nustatytos reikšmingos IRT rizikos kompetentingos institucijos turėtų vertinti, ar įstaiga taiko specialias šiai rizikai skirtas kontrolės priemones. Tolesniuose skirsniuose pateikiamas neišsamus konkrečių kontrolės priemonių sąrašas, į kurias reikėtų atsižvelgti vertinant pagal 3.2.3 skirsnį nustatytą reikšmingą riziką, priskirtą prie šių IRT rizikos kategorijų:

a. IRT prieinamumo ir tęstinumo rizika,
b. IRT saugumo rizika,
c. IRT pakeitimų rizika,
d. IRT duomenų vientisumo rizika,
e. IRT paslaugų pirkimo rizika.

(a) Reikšmingai IRT prieinamumo ir tęstinumo rizikai valdyti skirtos kontrolės priemonės

53. Be EBI SREP gairėse (279–281 punktuose) nustatytų reikalavimų, kompetentingos institucijos turėtų įvertinti, ar įstaiga taiko tinkamą IRT prieinamumo ir tęstinumo rizikos nustatymo, supratimo, vertinimo ir mažinimo sistemą.

54. Atlikdamos šį vertinimą kompetentingos institucijos pirmiausia turėtų atsižvelgti į tai, ar taikant šią sistemą:

a. nustatomi ypatingos svarbos IRT procesai ir susijusios pagalbinės IRT sistemos – jos turėtų būti įtrauktos į veiklos atsparumo ir tęstinumo planus kartu su:

   i. išsamia ypatingos svarbos veiklos procesų ir pagalbinių sistemų tarpusavio priklausomumo analize;

   ii. nustatytais pagalbinių IRT sistemų atkūrimo tikslais (pvz., paprastai juos kaip RTO ir RPO nustato įmonė ir (arba) jie nustatyti teisės aktuose);

   iii. tinkamu nenumatytų atvejų planavimu, kad, užtikrinus ypatingos svarbos IRT sistemų prieinamumą, tęstinumą ir atkūrimą, būtų galima kuo labiau sumažinti įstaigos veiklos sutrikimus ir jie neviršytų priimtinų ribų;

b. taikoma veiklos atsparumo, tęstinumo ir kontrolės aplinkos politika, standartai ir operacinės kontrolės priemonės, kurias sudaro:

   i. priemonės, kuriomis siekiama užtikrinti, kad vienas scenarijus, incidentas arba viena nelaimė nepaveiktų ir IRT gamybos, ir atkūrimo sistemų;

   ii. IRT sistemų atsarginių kopijų darymo, taip pat ypatingos svarbos programinės įrangos ir duomenų atkūrimo procedūros, kuriomis užtikrinamas šių atsarginių kopijų saugojimas saugioje ir pakankamai nutolusioje vietoje, kad šie ypatingos svarbos duomenys per incidentą arba nelaimę nebūtų sunaikinti arba pažeisti;

iii. sprendimų stebėsena siekiant laiku nustatyti su IRT prieinamumu arba tęstinumu susijusius incidentus;

iv. dokumentuotas incidentų valdymo ir pranešimų apie juos teikimo procesas, per kurį taip pat teikiamos gairės apie įvairias incidentų valdymo ir pranešimų apie juos teikimą ir atsakomybę, krizių valdymo komiteto (-ų) narius ir pavaldumo tvarką ekstremaliuoju atveju;

v. fizinės priemonės, kuriomis siekiama apsaugoti įstaigos ypatingos svarbos IRT infrastruktūrą (pvz., duomenų centrus) nuo aplinkos pavojų (pvz., potvynių ir kitų gaivalinių nelaimių) ir užtikrinti tinkamą IRT sistemų veikimo aplinką (pvz., oro kondicionavimą);

vi. procesai, pareigos ir atsakomybė, siekiant užtikrinti, kad tinkami veiklos atsparumo ir tęstinumo sprendimai bei planai taip pat būtų taikomi perkamoms IRT sistemoms ir paslaugoms;

vii. su IRT susijusių ypatingos svarbos IRT sistemų ir paslaugų rezultatų ir gebėjimų planavimo ir stebėsenos sprendimai kartu su apibrėžtais prieinamumo reikalavimais, kad būtų galima laiku nustatyti didelius rezultatų ir pajėgumų apribojimus;

viii. sprendimai, kuriais siekiama apsaugoti, jei reikia ir tinkama, ypatingos svarbos internetinę veiklą arba paslaugas (pvz., elektroninės bankininkystės paslaugas) nuo atkirtimo nuo paslaugos ir kitų internetu rengiamų kibernetinių išpuolių, kuriais siekiama sutrukdyti prieigą prie šios veiklos ir paslaugų arba ją sutrukdyti;

c. atliekami IRT prieinamumo ir tęstinumo sprendimų testai pagal įvairius tikroviškus scenarijus, įskaitant kibernetinius išpuolius, automatinio perjungimo ir ypatingos svarbos programinės įrangos ir duomenų atsarginių kopijų testai:

i. kurie yra planuojami, įforminami ir dokumentuojami, o remiantis jų rezultatais didinamas IRT prieinamumo ir tęstinumo užtikrinimo sprendimų veiksmingumas;

ii. į kuriuos įtraukiami organizacijos suinteresuotieji subjektai ir funkcijų vykdytojai, pvz., verslo linijos vadovybė, įskaitant veiklos tęstinumo, reagavimo į incidentus ir krizes komandas, taip pat susiję išoriniai ekosistemos suinteresuotieji subjektai;

iii. kuriuos atliekant tinkamai dalyvauja valdymo organas ir vyresnioji vadovybė (pvz., kaip krizių valdymo komandų nariai) ir kurių rezultatai pranešami šiam organui ir vadovybei.

(b) Reikšmingai IRT saugumo rizikai valdyti skirtos kontrolės priemonės

55. Kompetentingos institucijos turėtų vertinti, ar įstaiga taiko veiksmingą IRT saugumo rizikos nustatymo, supratimo, vertinimo ir mažinimo sistemą. Atlikdamos šį vertinimą kompetentingos institucijos pirmiausia turėtų atsižvelgti į tai, ar šioje sistemoje atsižvelgiama į:

a. aiškiai apibrėžtas pareigas ir atsakomybę, susijusias su:

i. asmenimi(s) ir (arba) komitetais, atsakingais ir (arba) atskaitingais už kasdienį IRT saugumo valdymą ir bendrosios IRT saugumo politikos parengimą, daug dėmesio skiriant reikiamam jų nepriklausomumui;

ii. IRT saugumo kontrolės priemonių rengimu, įgyvendinimu, valdymu ir stebėsena;
iii. ypatingos svarbos IRT sistemų ir paslaugų apsauga patvirtinant, pvz., pažeidžiamumo vertinimo procesą, programinės įrangos pataisų valdymą, prieigos taškų apsaugą (pvz., nuo virusinės kenkimo programos), įsilaužimo nustatymo ir prevencijos priemones;
iv. išorės arba vidaus IRT saugumo incidentų stebėsena, klasifikavimu ir valdymu, įskaitant reagavimą į incidentus ir IRT sistemų ir paslaugų atnaujinimą ir atkūrimą;
v. reguliariais ir aktyviais pavojų vertinimais, siekiant išlaikyti tinkamas saugumo kontrolės priemones;

b. taikomą IRT saugumo politiką, kuria atsižvelgiama ir prireikus laikomasi tarptautiniu lygmeniu pripažintų IRT saugumo standartų ir saugumo principų (pvz., prieigos teisių valdymui taikomo mažiausių privilegijų principo, pagal kurį prieiga apribojama tokiu būtiniausiu lygmeniu, kuriuo sudaromos sąlygos įprastiniam veikimui; saugumo struktūros projektavimui taikomo pakopinės apsaugos principo, pagal kurį kelių lygmenų saugumo mechanizmais didinamas visos sistemos saugumas);

c. procesą, pagal kurį nustatomos IRT sistemos, paslaugos ir tinkami saugumo reikalavimai, atitinkantys galimą sukčiavimo riziką, galimą netinkamą konfidencialių duomenų naudojimą ir (arba) piktnaudžiavimą jais, kartu su dokumentuotais saugumo lūkesčiais, kurių reikia laikytis dėl šių nustatytų IRT sistemų, paslaugų ir duomenų, kuris yra suderintas su įstaigos priimtina rizika ir kurio tinkamas įgyvendinimas stebimas;

d. dokumentuotą saugumo incidentų valdymo ir pranešimų apie juos teikimo procesą, per kurį teikiamos gairės apie įvairias incidentų valdymo ir pranešimų apie juos teikimo pareigas ir atsakomybę, krizių valdymo komiteto (-ų) narius ir pavaldumo tvarką su saugumu susijusiais ekstremaliaisiais atvejais;

e. naudotojų ir administracinės veiklos registravimą žurnaluose, kad būtų galima veiksmingai stebėti ir laiku nustatyti neteisėtą veiklą, imtis dėl jos atsakomųjų veiksmų, padėti atlikti arba vykdyti kriminalistinius saugumo incidentų tyrimus. Įstaiga turėtų taikyti registravimo žurnaluose politiką, kuria būtų apibrėžti tinkami tvarkytinų žurnalų tipai ir jų saugojimo laikotarpis;

f. informuotumo didinimo ir informavimo kampanijas arba iniciatyvas, kuriomis visais įstaigos lygmenimis siekiama teikti informaciją apie saugų įstaigos IRT sistemų naudojimą bei apsaugą ir apie pagrindinę IRT (ir kitą) saugumo riziką, apie kurią reikia žinoti, pirmiausia apie esamus ir kylančius kibernetinius pavojus (pvz., kompiuterių virusus, galimą išorinį arba vidinį piktnaudžiavimą arba išpuolius, kibernetinius išpuolius) ir vaidmenį mažinant saugumo pažeidimus;

g. tinkamas fizines saugumo priemones (pvz., apsauginę vaizdo stebėjimo sistemą, įsilaužimo signalizacijos įrangą, saugiąsias duris, siekiant užkirsti kelią neteisėtai fizinei prieigai prie ypatingos svarbos ir pažeidžiamų IRT sistemų (pvz., duomenų centrų);

h. priemones, kuriomis siekiama apsaugoti IRT sistemas nuo išpuolių, rengiamų naudojantis internetu (pvz., kibernetinių išpuolių) arba kitais išoriniais tinklais (pvz., įprastiniais telekomunikacijų ryšiais arba ryšiais su patikimais partneriais). Kompetentingos institucijos turėtų tikrinti, ar įstaigos sistemoje atsižvelgiama į:

i. procesą ir sprendimus, kuriais siekiama prižiūrėti išsamų ir atnaujintą duomenų aprašą ir apžvelgti visus į išorę nukreiptus tinklo ryšių taškus (pvz., svetaines, interneto taikomąsias

programas, belaidį vietinį tinklą, nuotolinę prieigą), per kurias į vidaus IRT sistemas galėtų įsilaužti trečiosios šalys;

ii. atidžiai valdomas ir stebimas saugumo priemones (pvz., užkardas, įgaliotuosius serverius, pašto perdavimą, antivirusines peržiūrinčiąsias ir turinio peržiūrėjimo programas), siekiant apsaugoti gaunamųjų ir išsiunčiamųjų duomenų srautą (pvz., el. laiškus) ir į išorę nukreiptus tinklo ryšius, per kuriuos trečiosios šalys galėtų įsilaužti į vidaus IRT sistemas;

iii. procesus ir sprendimus, kuriais siekiama apsaugoti svetaines ir taikomąsias programas, į kurias gali būti tiesiogiai taikomasi iš interneto ir (arba) išorės ir per kurias gali būti patenkama į vidaus IRT sistemas. Juos taikant, paprastai derinama pripažinta saugaus kūrimo praktika, IRT sistemų stiprinimo ir pažeidžiamumo peržiūros praktika ir (arba) įgyvendinami papildomi saugumo sprendimai, pvz., taikomųjų programų užkardų, įsilaužimo nustatymo ir (arba) įsilaužimo prevencijos sistemos;

iv. periodinį su įsiskverbimu susijusį saugumo testavimą, siekiant įvertinti įgyvendintų kibernetinių ir vidaus IRT saugumo priemonių ir procesų veiksmingumą. Šiuos testus turėtų atlikti reikiamos praktinės patirties turintys darbuotojai ir (arba) išorės ekspertai, o dokumentuoti testavimo rezultatai ir išvados turėtų būti pranešami vyresniajai vadovybei ir (arba) valdymo organui. Jei reikia ir taikoma, remdamasi šiais testais įstaiga turėtų išsiaiškinti, ar reikia toliau gerinti saugumo kontrolės priemones ir procesus ir (arba) gauti geresnį patikinimą dėl jų veiksmingumo.

(c) Reikšmingai IRT pakeitimų rizikai valdyti skirtos kontrolės priemonės

56. Kompetentingos institucijos turėtų vertinti, ar įstaiga taiko veiksmingą IRT pakeitimų rizikos nustatymo, supratimo, vertinimo ir mažinimo sistemą, atitinkančią įstaigos veiklos pobūdį, mastą, sudėtingumą ir IRT rizikos profilį. Įstaigos sistema turėtų apimti riziką, susijusią su IRT sistemų pakeitimų rengimu, testavimu ir patvirtinimu, įskaitant programinės įrangos kūrimą arba keitimą, prieš šias sistemas perkeliant į gamybos aplinką, ir šia sistema turėtų būti užtikrinamas tinkamas IRT gyvavimo ciklo valdymas. Atlikdamos šį vertinimą kompetentingos institucijos pirmiausia turėtų atsižvelgti į tai, ar šioje sistemoje atsižvelgiama į:

a. dokumentuojamus procesus, kuriais valdomi ir kontroliuojami IRT sistemų pakeitimai (pvz., konfigūravimo ir pataisų valdymas) bei duomenų pakeitimai (pvz., klaidų taisymas arba duomenų tikslinimas) ir užtikrinamas tinkamas IRT rizikos vadovybės dalyvavimas atliekant svarbius IRT pakeitimus, galinčius turėti reikšmingos įtakos įstaigos rizikos profiliui arba pozicijai;

b. specifikacijas, susijusias su reikiamu pareigų atskyrimu įvairiais įgyvendinamų IRT keitimo procesų etapais (pvz., sprendimų projektavimo ir plėtojimo, naujos programinės įrangos ir (arba) pakeitimų testavimo ir patvirtinimo, perkėlimo ir įgyvendinimo gamybos aplinkoje, klaidų taisymo), atkreipiant dėmesį į įgyvendintus sprendimus ir pareigų atskyrimą, siekiant valdyti ir kontroliuoti IRT darbuotojų (pvz., kūrėjų, IRT sistemų administratorių, duomenų bazių administratorių) arba kitos šalies (pvz., verslo naudotojų, paslaugų teikėjų) atliekamus gamybos IRT sistemų ir duomenų pakeitimus;

c. testavimo aplinkas, kuriomis tinkamai atsižvelgiama į gamybos aplinkas;

d. esamų gamybos, testavimo ir kūrimo aplinkose veikiančių taikomųjų programų ir IRT sistemų turto aprašą, kad būtų galima tinkamai valdyti, įgyvendinti ir stebėti reikiamus susijusių IRT sistemų pakeitimus (pvz., versijų naujinimą arba naujovinimą, sistemų taisymą, konfigūracijos pakeitimus);

e. naudojamų IRT sistemų gyvavimo ciklo stebėsenos ir valdymo procesą, siekiant užtikrinti, kad šios sistemos toliau atitiktų ir palaikytų faktinės veiklos ir rizikos valdymo reikalavimus, kad naudojamus IRT sprendimus ir sistemas vis dar prižiūrėtų jų pardavėjai ir kad būtų taikomos pagalbinės tinkamos programinės įrangos kūrimo ciklo (angl. SDLC) procedūros;

f. programinės įrangos pirminio teksto kontrolės sistemą ir atitinkamas procedūras, kuriomis siekiama išvengti neteisėtų vietoje sukurtos programinės įrangos pirminio teksto pakeitimų;

g. procesą, per kurį atliekama naujų arba reikšmingai pakeistų IRT sistemų ir programinės įrangos saugumo ir pažeidžiamumo patikra, prieš išleidžiant jas į gamybos aplinką ir aplinką, kurioje jos gali tapti kibernetinių išpuolių taikiniu;

h. procesus ir sprendimus, kuriais siekiama išvengti neteisėto arba netyčinio konfidencialių duomenų atskleidimo pakeičiant, archyvuojant, šalinant arba naikinant IRT sistemas;

i. nepriklausomus patikros ir patvirtinimo procesus, kuriais siekiama sumažinti riziką, susijusią su žmonių klaidomis atliekant IRT sistemų pakeitimus, galinčiomis turėti didelį neigiamą poveikį įstaigos veiklos prieinamumui, tęstinumui arba saugumui (pvz., atliekant didelius užkardos konfigūracijos pakeitimus) arba įstaigos saugumui (pvz., atliekant užkardų pakeitimus).

(d) Reikšmingai IRT duomenų vientisumo rizikai valdyti skirtos kontrolės priemonės

57. Kompetentingos institucijos turėtų vertinti, ar įstaiga taiko veiksmingą IRT duomenų vientisumo rizikos nustatymo, supratimo, vertinimo ir mažinimo sistemą, atitinkančią įstaigos veiklos pobūdį, mastą, sudėtingumą ir IRT rizikos profilį. Įstaigos sistema turėtų būti atsižvelgiama į riziką, susijusią su IRT sistemose saugomų ir jomis apdorojamų duomenų vientisumo išsaugojimu. Atlikdamos šį vertinimą kompetentingos institucijos pirmiausia turėtų atsižvelgti į tai, ar šioje sistemoje atsižvelgiama į:

a. politiką, kuria apibrėžiamos IRT sistemose saugomų duomenų vientisumo valdymo pareigos ir atsakomybė (pvz., duomenų architektūros projektuotojo, duomenų pareigūnų [6], duomenų patikėtinių[7], duomenų savininkų ir (arba) tvarkytojų[8]) ir teikiamos gairės apie tai, kurie duomenys yra itin svarbūs duomenų vientisumo atžvilgiu ir todėl jiems įvairiuose IRT duomenų gyvavimo ciklo etapuose turėtų būti taikomos specialios IRT kontrolės priemonės (pvz., automatizuotos įvesties patvirtinimo kontrolės priemonės, duomenų perdavimo kontrolės priemonės, derinimas ir pan.) arba patikros (pvz., suderinamumo su duomenų architektūra patikra);

b. kartu su susijusiais veiklos ir IT suinteresuotaisiais subjektais patvirtintą dokumentuotą duomenų architektūrą, duomenų modelį ir (arba) žodyną, siekiant remti reikiamą duomenų nuoseklumą IRT sistemose ir užtikrinti, kad duomenų architektūra, duomenų modelis ir (arba) žodynas išliktų suderinti su veiklos ir rizikos valdymo poreikiais;

[6] Duomenų pareigūnas atsako už duomenų apdorojimą ir naudojimą.
[7] Duomenų patikėtinis atsako už saugų duomenų deponavimą, transportavimą ir saugojimą.
[8] Duomenų tvarkytojas atsako už duomenų elementų – turinio ir metaduomenų – valdymą ir tinkamumą.

c. politiką, susijusią su leidžiamu galutinių naudotojų kompiuterių naudojimu ir pasikliovimu jais, pirmiausia susijusią su svarbių galutinių naudotojų kompiuterijos sprendimų nustatymu, registravimu ir dokumentavimu (pvz., apdorojant svarbius duomenis) ir tikėtinais saugumo lygiais, siekiant užkirsti kelią neteisėtoms priemonės ir joje saugomų duomenų modifikacijoms;

d. dokumentuotus išimčių valdymo procesus, siekiant spręsti nustatytas IRT duomenų vientisumo problemas, atsižvelgiant į šių duomenų svarbą ir neskelbiamumą.

58. Dėl prižiūrimų įstaigų, patenkančių į BBPK 239 veiksmingo rizikos duomenų apibendrinimo ir pranešimo apie riziką principų[9] taikymo sritį, kompetentingos institucijos turėtų tikrinti įstaigos rizikos analizę, susijusią su pranešimo apie riziką ir rizikos duomenų apibendrinimo pajėgumais, palyginti su principais ir parengtais susijusiais dokumentais, atsižvelgdama į šių principų įgyvendinimo tvarkaraštį ir pereinamojo laikotarpio nuostatas.

(e) Reikšmingai IRT paslaugų pirkimo rizikai valdyti skirtos kontrolės priemonės

59. Kompetentingos institucijos turėtų vertinti, ar įstaigos paslaugų pirkimo strategija, laikantis Europos bankininkystės priežiūros institucijų komiteto (EBPIK) paslaugų pirkimo gairių (2006) reikalavimų ir EBI SREP gairių 85 punkto d papunkčio reikalavimų, tinkamai taikoma IRT paslaugų pirkimui, įskaitant paslaugų pirkimą iš IRT paslaugas grupėje teikiančių subjektų. Vertindamos IRT paslaugų pirkimo riziką, kompetentingos institucijos turėtų atsižvelgti į tai, kad, siekiant išvengti darbo dubliavimosi arba dvigubos apskaitos, IRT paslaugų pirkimo rizika gali būti įtraukta į būdingos operacinės rizikos vertinimą pagal EBI SREP gairių 240 punkto j papunktį.

60. Kompetentingos institucijos konkrečiai turėtų vertinti, ar įstaiga taiko veiksmingą IRT paslaugų pirkimo rizikos nustatymo, supratimo ir vertinimo sistemą, pirmiausia – ar ji taiko kontrolės priemones ir kontrolės aplinką, kuriomis siekiama mažinti su reikšmingomis perkamomis IRT paslaugomis susijusią riziką, kurios atitinka įstaigos dydį, veiklą ir IRT rizikos profilį ir kurias sudaro:

a. su paslaugų teikėjų (pvz., debesijos paslaugų teikėjų) pasitelkimu ir naudojimusi jų paslaugomis susijusio IRT paslaugų pirkimo poveikio įstaigos rizikos valdymui vertinimas, kuris yra dokumentuojamas ir į kurį vyresnioji vadovybė arba valdymo organas atsižvelgia priimdama(s) sprendimą dėl to, ar pirkti paslaugas. Įstaiga turėtų tikrinti paslaugų teikėjo IRT rizikos valdymo politiką, IRT kontrolės priemones ir kontrolės aplinką siekdama įsitikinti, kad jos atitinka įstaigos vidaus rizikos valdymo tikslus ir norimą prisiimti riziką. Ši patikra sutartiniu paslaugų pirkimo laikotarpiu turėtų būti periodiškai naujinama, atsižvelgiant į perkamų paslaugų ypatybes;

b. sutartiniu paslaugų pirkimo laikotarpiu atliekama perkamų paslaugų IRT rizikos stebėsena, kuri yra įtraukta į įstaigos rizikos valdymą ir kuria remiamasi teikiant įstaigos IRT rizikos valdymo ataskaitas (pvz., veiklos tęstinumo ataskaitas, saugumo ataskaitas);

c. gautų paslaugų lygių stebėsena ir lyginimas su sutartyje nustatytais paslaugų lygiais, kurie turėtų būti įtraukti į paslaugų pirkimo sutartį arba susitarimą dėl paslaugų lygio;

[9] Bazelio bankų priežiūros komiteto dokumentas *Principles for effective risk data aggregation and risk reporting* (Veiksmingo rizikos duomenų apibendrinimo ir pranešimo apie riziką principai), 2013 m. sausio mėn., paskelbta internetu adresu http://www.bis.org/publ/bcbs239.pdf.

d. tinkamas personalas, ištekliai ir kompetencijos, kad būtų galima stebėti ir valdyti perkamų paslaugų IRT riziką.

3.4 Išvadų apibendrinimas ir balo skyrimas

61. Atlikusios pirmiau nurodytą vertinimą, kompetentingos institucijos turėtų susidaryti nuomonę apie įstaigos IRT riziką. Ši nuomonė turėtų būti išdėstoma išvadų santraukoje, į kurią kompetentingos institucijos turėtų atsižvelgti skirdamos operacinės rizikos balą pagal EBI SREP gairių 6 lentelę. Savo nuomonę kompetentingos institucijos turėtų grįsti reikšminga IRT rizika, atsižvelgdamos į toliau išvardytus į operacinės rizikos vertinimą įtrauktinus analizės kriterijus.

a. Rizikos analizės kriterijai:

   i. įstaigos IRT rizikos profilis ir pozicijos;
   ii. nustatytos ypatingos svarbos IRT sistemos ir paslaugos;
   iii. IRT rizikos reikšmingumas ypatingos svarbos IRT sistemų atžvilgiu.

b. Valdymo ir kontrolės analizės kriterijai:

   i. ar įstaigos IRT rizikos valdymo politika ir strategija dera su jos bendrąja strategija ir norima prisiimti rizika;
   ii. ar organizacijos IRT rizikos valdymo sistema yra patikima, joje aiškiai apibrėžtos atsakomybės sritys ir aiškiai atskirtos už riziką atsakingų asmenų ir valdymo bei kontrolės funkcijų vykdytojų užduotys;
   iii. ar taikomos tinkamos IRT rizikos vertinimo, stebėsenos ir ataskaitų teikimo sistemos;
   iv. ar taikomos tinkamos reikšmingos IRT rizikos kontrolės sistemos.

62. Jei kompetentingos institucijos laiko IRT riziką reikšminga ir nusprendžia vertinti šią riziką kaip operacinės rizikos pakategorę bei skirti jai balą, jos gali naudotis toliau pateikta analizės kriterijų, pagal kuriuos skiriamas IRT rizikos balas, lentele (1 lentele).

1 lentelė. Priežiūriniai analizės kriterijai, pagal kuriuos skiriamas IRT rizikos balas

Rizikos balas	Priežiūros institucijos nuomonė	Būdingos rizikos analizės kriterijai	Tinkamo valdymo ir kontrolės priemonių analizės kriterijai
1	Atsižvelgiant į būdingos rizikos lygį, valdymą ir kontrolės priemones, reikšmingo prudencinio poveikio įstaigai rizikos nepastebima.	• Remiantis informacijos šaltiniais, į kuriuos reikia atsižvelgti pagal 37 punktą, reikšmingų IRT rizikos pozicijų nematyti. • Įvertinus įstaigos IRT rizikos profilio pobūdį, taip pat patikrinus ypatingos svarbos IRT sistemas ir IRT sistemoms bei paslaugoms kylančią reikšmingą IRT riziką, reikšmingos IRT rizikos nenustatyta.	• Įstaigos IRT rizikos politika ir strategija atitinka įstaigos bendrąją strategiją ir norimą prisiimti riziką. • Organizacijos IRT rizikos sistema yra patikima, joje aiškiai apibrėžtos atsakomybės sritys ir aiškiai atskirtos už riziką atsakingų asmenų ir valdymo bei kontrolės funkcijų vykdytojų užduotys. • Taikomos tinkamos IRT rizikos vertinimo, stebėsenos ir ataskaitų teikimo sistemos. • Taikoma tinkama IRT rizikos kontrolės sistema.
2	Atsižvelgiant į būdingos rizikos lygį, valdymą ir kontrolės priemones, kyla maža reikšmingo prudencinio poveikio įstaigai rizika.	• Remiantis informacijos šaltiniais, į kuriuos reikia atsižvelgti pagal 37 punktą, reikšmingų IRT rizikos pozicijų nematyti. • Įvertinus įstaigos IRT rizikos profilio pobūdį, taip pat patikrinus ypatingos svarbos IRT sistemas ir IRT sistemoms bei paslaugoms kylančią reikšmingą IRT riziką, nustatyta nedidelė IRT rizikos pozicija (pvz., ne daugiau kaip dvi iš penkių iš anksto apibrėžtų IRT rizikos kategorijų).	
3	Atsižvelgiant į būdingos rizikos lygį, valdymą ir kontrolės priemones, kyla vidutinė prudencinio poveikio įstaigai rizika.	• Remiantis informacijos šaltiniais, į kuriuos reikia atsižvelgti pagal 37 punktą, nustatyta galimų reikšmingų IRT rizikos pozicijų požymių. • Įvertinus įstaigos IRT rizikos profilio pobūdį, taip pat patikrinus ypatingos svarbos IRT sistemas ir IRT sistemoms bei paslaugoms kylančią reikšmingą IRT riziką, nustatyta padidėjusi IRT rizikos pozicija (pvz., trys arba daugiau iš penkių iš anksto apibrėžtų IRT rizikos kategorijų).	
4	Atsižvelgiant į būdingos rizikos lyg, valdymą ir kontrolės	• Remiantis informacijos šaltiniais, į kuriuos reikia atsižvelgti pagal 37 punktą, nustatyti keli reikšmingų	

	priemones, kyla didelė reikšmingo prudencinio poveikio įstaigai rizika.	IRT rizikos pozicijų požymiai. • Įvertinus įstaigos IRT rizikos profilio pobūdį, taip pat patikrinus ypatingos svarbos IRT sistemas ir IRT sistemoms bei paslaugoms kylančią reikšmingą IRT riziką, nustatyta didelė IRT rizikos pozicija (pvz., keturios arba penkios iš penkių iš anksto apibrėžtų IRT rizikos kategorijų).	

Priedas. IRT rizikos klasifikacija

Penkios IRT rizikos kategorijos ir neišsamus IRT rizikos, galinčios turėti didelio masto ir (arba) operacinį, reputacinį ar finansinį poveikį, sąrašas

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
IRT prieinamumo ir tęstinumo rizika	Netinkamas pajėgumų valdymas	Trūkstant išteklių (pvz., techninės, programinės įrangos, darbuotojų, paslaugų teikėjų) gali būti neįmanoma pritaikyti paslaugos, kad būtų galima atsižvelgti į veiklos poreikius, sistemų sutrikimus, paslaugos kokybės suprastėjimą ir (arba) operacines klaidas.	• Pajėgumų trūkumas gali turėti įtakos perdavimo greičiui ir tinklo (interneto) prieinamumui naudojantis tokioms paslaugoms kaip internetinė bankininkystė. • (Vidaus arba trečiosios šalies) darbuotojų trūkumas gali lemti sistemų sutrikimus ir (arba) operacines klaidas.
	IRT sistemų gedimai	Neprieinamumas dėl techninės įrangos gedimų.	• Atminties įtaisų (standžiųjų diskų), serverio arba kitos IRT įrangos gedimas ir (arba) netinkamas veikimas, pvz., dėl nepakankamos techninės priežiūros.
		Neprieinamumas dėl programinės įrangos gedimų ir klaidų.	• Dėl taikomosios programos programinės įrangos begalinio ciklo negalima įvykdyti operacijos. • Atjungimas tebenaudojant pasenusias IRT sistemas ir sprendimus, kurie nebeatitinka aktualių prieinamumo ir atsparumo reikalavimų ir (arba) kurių nebeprižiūri jų pardavėjai.
	Netinkamas IRT tęstinumo ir atkūrimo po nelaimių planavimas	Neveikiantys po incidento suaktyvinti IRT planuoto prieinamumo ir (arba) tęstinumo užtikrinimo sprendimai ir (arba) atkūrimas po nelaimių (pvz., atsarginis atkūrimo duomenų centras).	• Dėl skirtingos pirminio ir antrinio duomenų centrų konfigūracijos atsarginiu duomenų centru gali būti neįmanoma užtikrinti planuoto paslaugos tęstinumo.
	Trikdomieji ir naikinamieji kibernetiniai	Įvairiais (pvz., aktyvizmo, šantažo) tikslais rengiami išpuoliai, dėl kurių perkraunamos sistemos ir tinklas, todėl teisėti naudotojai negali naudotis internetinėmis	• Paskirstytosios paslaugos trikdymo atakos (angl. *Distributed Denial of Service*, *DDoS*) vykdomos

[10] IRT rizika nurodyta toje rizikos kategorijoje, kuriai ji daro didžiausią poveikį, bet ji gali daryti poveikį ir kitoms rizikos kategorijoms.

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
	išpuoliai	kompiuterinėmis paslaugomis.	naudojant daugybę internete esančių kompiuterinių sistemų, kurias valdo programišiai ir kuriomis į internetines (pvz., elektroninės bankininkystės) paslaugas išsiunčiama daugybė tariamai teisėtų paslaugų užklausų.
IRT saugumo rizika	Kibernetiniai ir kiti išoriniai su IRT susiję išpuoliai	Įvairiais (pvz., sukčiavimo, šnipinėjimo, aktyvizmo ir (arba) sabotažo, kibernetinio terorizmo) tikslais įvairiais metodais (pvz., socialinės inžinerijos, bandant įsilaužti išnaudojant silpnąsias vietas, naudojant kenkimo programinę įrangą) iš interneto arba išorinių tinklų rengiami išpuoliai, per kuriuos perimamas vidaus IRT sistemų valymas.	Įvairių rūšių išpuoliai: • išplėstinė nuolatinė grėsmė (angl. *Advanced Persistent Threat*, APT), kad gali būti perimtas vidaus sistemų valdymas arba pavagiama informacija (pvz., su tapatybės vagyste susijusi informacija, kredito kortelių informacija); • kenkimo programinė įranga (pvz., išpirkos reikalaujanti programinė įranga), kuria duomenys užšifruojami šantažo tikslais; • vidaus IRT sistemų užkrėtimas Trojos arkliais, siekiant slaptai vykdyti kenksmingus sistemos veiksmus; • IRT sistemos ir (arba) saityno, taikomosios programos pažeidžiamumo išnaudojimas (pvz., SQL injekcija ir pan.) siekiant įgyti prieigą prie vidaus IRT sistemos.
		Programišių vykdomos apgaulingos mokėjimo operacijos įsilaužus į elektroninės bankininkystės ir mokėjimo paslaugas arba apėjus jų saugumo priemones ir (arba) taikantis į įstaigos vidaus mokėjimo sistemų saugumo pažeidžiamumą arba šiuo pažeidžiamumu pasinaudojant.	• Išpuoliai prieš elektroninės bankininkystės arba mokėjimo paslaugas siekiant vykdyti neteisėtas operacijas. • Apgaulingų mokėjimo operacijų sukūrimas ir išsiuntimas iš įstaigos vidaus mokėjimo sistemų (pvz., apgaulingi SWIFT pranešimai).
		Programišių vykdomos apgaulingos vertybinių popierių operacijos įsilaužus į elektroninės bankininkystės paslaugas arba apėjus jų saugumo priemones, taip pat įgyjant prieigą prie kliento vertybinių popierių sąskaitų.	• Kainų išpūtimo ir pardavimo išpuoliai, kuriuos vykdydami išpuolių rengėjai įgyja prieigą prie klientų elektroninės bankininkystės vertybinių popierių sąskaitų ir teikia apgaulingus pirkimo arba pardavimo užsakymus, siekdami paveikti rinkos

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
			kainą ir (arba) pasipelnyti remiantis pirmiau nustatytomis vertybinių popierių pozicijomis.
		Taikymasis į bet kokių IRT sistemų komunikacijos ryšius ir pokalbius siekiant rinkti informaciją ir (arba) vykdyti sukčiavimą.	• Neteisėtos informacijos ir (arba) neapsaugotų grynuoju tekstu perduodamų tapatumo nustatymo duomenų perėmimas.
	Nepakankamas vidinis IRT saugumas	Neteisėtos prieigos prie ypatingos svarbos IRT sistemų įgijimas iš įstaigos įvairiais tikslais (pvz., sukčiavimo, kenkėjiškos prekybinės veiklos ir slėpimo, duomenų vagystės, aktyvizmo ir (arba) sabotažo) įvairiais metodais (pvz., piktnaudžiaujant privilegijomis ir (arba) jas išplečiant, pavogus tapatybės duomenis, naudojantis socialine inžinerija, išnaudojant IRT sistemų pažeidžiamumą, naudojant kenkimo programinę įrangą).	• Klavišų paspaudimų registravimo programinės įrangos įdiegimas siekiant pavogti naudotojo identifikatorius ir slaptažodžius, kad būtų galima įgyti neteisėtą prieigą prie konfidencialių duomenų ir (arba) vykdyti sukčiavimą. • Nesaugių slaptažodžių nulaužimas / atspėjimas siekiant įgyti neteisėtas arba aukštesnio lygmens prieigos teises. • Sistemos administratoriaus vykdomas sukčiavimas naudojantis operacinėmis sistemomis arba duomenų bazių infrastruktūra (siekiant tiesiogiai modifikuoti duomenų bazes).
		Neteisėta IRT manipuliacija dėl netinkamų IRT prieigos valdymo procedūrų ir praktikos.	• Nereikalingų paskyrų, pvz., darbuotojų, kurių pareigos pasikeitė ir (arba) kurie išėjo iš įstaigos, įskaitant svečius arba tiekėjus, kuriems nebereikia prieigos, paskyrų neišjungimas arba nepanaikinimas ir kartu neteisėtos prieigos suteikimas prie IRT sistemų. • Pernelyg plačių prieigos teisių ir privilegijų suteikimas ir kartu neteisėtos prieigos suteikimas ir (arba) sąlygų nuslėpti kenkėjišką veiklą sudarymas.
		Saugumo pavojai dėl to, kad darbuotojai nepakankamai informuoti apie saugumą, todėl nesupranta IRT saugumo politikos ir procedūrų, jų nepaiso arba nesilaiko.	• Klysdami darbuotojai padeda vykdyti išpuolį (t. y. socialinė inžinerija). • Netinkama su prieigos duomenimis susijusi praktika: slaptažodžių dalijimasis, lengvai atspėjamų

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
			slaptažodžių naudojimas, to paties slaptažodžio naudojimas daugeliu įvairių tikslų ir pan. • Neužšifruotų konfidencialių duomenų laikymas nešiojamuose kompiuteriuose ir nešiojamosiose duomenų laikmenose (pvz., USB raktuose), kurios gali būti pametamos arba pavagiamos.
		Neteisėtas konfidencialios informacijos saugojimas ne įstaigoje arba perdavimas iš įstaigos.	• Konfidencialios informacijos vogimas arba tyčinis nutekinimas ar perdavimas neįgaliotiesiems asmenims arba paviešinimas.
	Nepakankamas fizinis IRT saugumas	Netinkamai naudojant IRT turtą arba jį pavagiant pasinaudojus fizine prieiga padaroma žala, prarandamas turtas ar duomenys arba sudaromos sąlygos kitiems pavojams.	• Fizinis įsilaužimas į biurų pastatus ir (arba) duomenų centrus siekiant pavogti IRT įrangą (pvz., stalinius, nešiojamus kompiuterius, laikmenas) ir (arba) nukopijuoti duomenis pasinaudojus fizine prieiga prie IRT sistemų.
		Tyčinė arba atsitiktinė žala fiziniam IRT turtui dėl terorizmo, nelaimingų atsitikimų arba netinkamo / klaidingo įstaigos ir (arba) trečiųjų šalių (tiekėjų, remontininkų) atlikto manipuliavimo.	• Fizinis terorizmas (t. y. teroristų vykdomi sprogdinimai) arba IRT turto sabotažas. • Duomenų centro sunaikinimas per gaisrą, dėl vandens nuotėkio ir kitų veiksnių.
		Nepakankama fizinė apsauga nuo gaivalinių nelaimių, per kurias iš dalies arba visiškai sunaikinamos IRT sistemos ir (arba) duomenų centrai.	• Žemės drebėjimai, didelis karštis, audros, stiprios pūgos, potvyniai, gaisras, žaibas.
IRT pakeitimų rizika	Netinkamos IRT sistemų pakeitimų ir IRT plėtros kontrolės priemonės	Incidentai dėl neaptiktų klaidų arba pažeidžiamumo atlikus, pvz., programinės įrangos, IRT sistemų ir duomenų, pakeitimą (pvz., nenumatytas pakeitimo poveikis arba prastai valdomas pakeitimas, nes neatliekamas pakankamas testavimas arba taikoma netinkama pakeitimų valdymo praktika).	• Nepakankamai išbandytos programinės įrangos išleidimas į gamybos aplinką arba konfigūracijos pakeitimai, kurie netikėtai neigiamai veikia duomenis (pvz., juos pažeidžia, pašalina) ir (arba) IRT sistemų veikimą (pvz., ji sugenda, ima prasčiau veikti). • Nevaldomi IRT sistemų arba duomenų pakeitimai gamybos aplinkoje. • Išleidus prastai apsaugotas IRT sistemas arba taikomąsias interneto programas į gamybos aplinką, programišiai įgyja galimybių vykdyti išpuolius prieš

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
			teikiamas internetines paslaugas ir (arba) įsilaužti į vidaus IRT sistemas. • Nevaldomi viduje sukurtos programinės įrangos pirminio teksto pakeitimai. • Nepakankamas testavimas dėl nesukurtos tinkamos testavimo aplinkos.
	Netinkama IRT architektūra	Dėl prasto IRT architektūros valdymo projektuojant, diegiant ir prižiūrint IRT sistemas (pvz., programinę, techninę įrangą ar duomenis) laikui bėgant gali susidaryti sudėtingos, sunkios taikyti ir brangiai valdomos IRT sistemos, kurios gali nebebūti pakankamai suderintos su veiklos poreikiais ir neatitikti aktualių rizikos valdymo reikalavimų.	• Ilgesnį laiką netinkamai valdant IRT sistemų, programinės įrangos ir (arba) duomenų pakeitimus, gali susidaryti sudėtingos, skirtingos ir sunkiai valdomos IRT sistemos ir architektūra, galinčios lemti įvairų neigiamą poveikį veiklai ir rizikos valdymui (pvz., nepakankamą lankstumą ir aktyvumą, IRT incidentus ir gedimus, dideles veiklos sąnaudas, mažesnį IRT saugumą ir atsparumą, prastesnę duomenų kokybę ir mažesnius pranešimo gebėjimus). • Pernelyg išsamiai pritaikant ir išplečiant komercinės programinės įrangos paketus viduje sukurta programine įranga, ateityje nebesugebama įgyvendinti komercinės programinės įrangos laidų ir naujinių ir kyla rizika, kad pardavėjas jos nebeprižiūrės.
	Netinkamas gyvavimo ciklo ir pataisų valdymas	Netinkamai tvarkomas viso IRT turto aprašas, kuriuo turėtų būti remiamas arba su kuriuo turėtų būti derinamas tinkamas gyvavimo ciklo ir pataisų valdymas. Dėl to IRT sistemos nepakankamai taisomos (todėl yra pažeidžiamesnės), pasensta ir gali nebeatitikti veiklos bei rizikos valdymo poreikių.	• Nepataisytos ir pasenusios IRT sistemos, galinčios daryti neigiamą poveikį veiklos ir rizikos valdymui (pvz., nepakankamas lankstumas ir aktyvumas, IRT atjungimas, mažesnis IRT saugumas ir atsparumas).
IRT duomenų vientisumo rizika	Prastas IRT duomenų apdorojimas arba tvarkymas	Dėl sistemos, ryšio ir (arba) taikomosios programos klaidų, gedimų arba netinkamo duomenų išgavimo, perdavimo ir įkėlimo proceso gali būti pažeisti arba prarasti duomenys.	• Su paketiniu apdorojimu susijusi IT sistemos klaida, dėl kurios kliento bankų sąskaitose rodomi netikslūs likučiai. • Netinkamai vykdomos užklausos.

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
			• Duomenų praradimas įvykus duomenų dubliavimo (atsarginės kopijos darymo) klaidai.
	Netinkamai suprojektuotos IRT sistemose taikomos duomenų patvirtinimo kontrolės priemonės	Klaidos, susijusios su trūkstamomis arba neveiksmingomis automatizuotos duomenų įvesties ir priėmimo kontrolės priemonėmis (pvz., taikomomis trečiųjų šalių duomenims), duomenų perdavimu, IRT sistemose taikomomis apdorojimo ir išvesties kontrolės priemonėmis (pvz., įvesties galiojimo kontrolės priemonėmis, duomenų derinimu).	• Nepakankamas arba netinkamas duomenų įvesties formatavimas ir (arba) patvirtinimas taikomosiose programose ir (arba) naudotojų sąsajose. • Netaikomos išvesties duomenų derinimo kontrolės priemonės. • Netaikomos įvykdytų duomenų išgavimo procesų (pvz., duomenų bazių užklausų) kontrolės priemonės, todėl susidaro klaidingų duomenų. • Netinkamų išorinių duomenų naudojimas.
	Prastai kontroliuojami duomenų pakeitimai gamybos IRT sistemose	Duomenų klaidos, atsirandančios dėl to, kad nepakankamai kontroliuojamas gamybos IRT sistemose atliekamo duomenų manipuliavimo tinkamumas ir pagrįstumas.	• Kūrėjai ir duomenų bazių administratoriai naudojasi tiesiogine prieiga ir nekontroliuojamai keičia duomenis gamybos IRT sistemose, pvz., įvykus IRT incidentui.
	Prastas duomenų architektūros, duomenų srautų, duomenų modelių arba duomenų žodynų projektavimas ir (arba) valdymas	Prastai valdant duomenų architektūrą, duomenų modelius, duomenų srautus arba duomenų žodynus, IRT sistemose gali atsirasti kelios tų pačių duomenų versijos, kurioms trūksta nuoseklumo dėl skirtingai taikomų duomenų modelių arba duomenų apibrėžčių, ir (arba) gali atsirasti pagrindinės duomenų kartos ir pakeitimų proceso skirtumų.	• Naudojant skirtingas kiekvieno produkto arba veiklos skyriaus klientų duomenų bazes, kurioms taikomos skirtingos duomenų apibrėžtys ir sritys, visos finansų įstaigos arba grupės lygmeniu atsiranda nesuderintų, sunkiai palyginamų ir sunkiai integruojamų klientų duomenų.
IRT paslaugų pirkimo rizika	Nepakankamas trečiosios šalies arba kito grupės subjekto paslaugų atsparumas	Ypatingos svarbos perkamų IRT paslaugų, telekomunikacijos ir komunalinių paslaugų neprieinamumas. Paslaugų teikėjui patikėtų ypatingos svarbos ir (arba) neskelbtinų duomenų praradimas arba pažeidimas.	• Pagrindinių paslaugų neprieinamumas dėl iš tiekėjų perkamų IRT sistemų arba taikomųjų programų gedimų. • Telekomunikacijų linijų veikimo sutrikimas. • Nepakankamas elektros energijos tiekimas.
	Netinkamas paslaugų pirkimo	Labai suprastėjusi paslaugų kokybė arba paslaugų sutrikimai dėl to, kad tiekėjas, iš kurio perkamos	• Dėl prastų incidentų valdymo procedūrų, sutartinių kontrolės mechanizmų ir į paslaugų teikėjo sutartį

IRT rizikos kategorijos	IRT rizika (sąrašas neišsamus)[10]	Rizikos aprašas	Pavyzdžiai
	valdymas	paslaugos, yra netinkamai pasirengęs arba taiko neveiksmingus kontrolės procesus. Netinkamai valdant paslaugų pirkimą, gali trūkti tinkamų IRT rizikos nustatymo, įvertinimo, sumažinimo, stebėsenos gebėjimų bei pajėgumų ir gali sumažėti įstaigos operaciniai gebėjimai.	įtrauktų garantijų didėja svarbių darbuotojų priklausomybė nuo trečiųjų šalių ir pardavėjų. • Dėl netinkamų su paslaugų teikėjo IRT aplinka susijusių pakeitimų valdymo kontrolės priemonių gali labai suprastėti paslaugų kokybė arba atsirasti didelių sutrikimų.
	Netinkamas trečiosios šalies arba kito grupės subjekto saugumas	Įsilaužimas į trečiosios šalies paslaugos teikėjų IRT sistemas, darantis tiesioginį poveikį perkamoms paslaugoms arba ypatingos svarbos ir (arba) konfidencialiems pas paslaugos teikėją saugomiems duomenims. Neteisėta paslaugų teikėjo darbuotojų prieiga prie ypatingos svarbos ir (arba) neskelbtinų pas paslaugų teikėją saugomų duomenų.	• Nusikaltėlių arba teroristų įsilaužimas pas paslaugų teikėjus siekiant prieiti prie įstaigos IRT sistemų arba pas paslaugų teikėją saugomų ypatingos svarbos arba neskelbtinų duomenų ir (arba) šiuos duomenis sunaikinti. • Piktavališki paslaugų teikėjo asmenys stengiasi pavogti ir parduoti neskelbtinus duomenis.