Gairės

EBA/GL/2019/04

2019 m. lapkričio 28 d.

EBI IRT ir saugumo rizikos valdymo gairės

Atitiktis gairėms ir informavimo pareiga

Šių gairių statusas

1. Šiame dokumente pateiktos pagal Reglamento (ES) Nr. 1093/2010[1] 16 straipsnį parengtos gairės. Pagal Reglamento (ES) 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 Europos 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 yra visų pirma skiriamos įstaigoms.

Pranešimo reikalavimai

3. Pagal Reglamento (ES) Nr. 1093/2010 16 straipsnio 3 dalį kompetentingos institucijos ne vėliau kaip ([... m. ... ... d.]) privalo EBI pranešti, ar laikosi arba ketina laikytis šių gairių, arba nurodyti nesilaikymo priežastis. Jeigu kompetentingos institucijos iki šio termino nepateikia jokio pranešimo, EBI laiko, kad kompetentingos institucijos gairių nesilaiko. Pranešimus reikėtų siųsti adresu compliance@eba.europa.eu užpildžius EBI interneto svetainėje pateiktą formą ir įrašius nuorodą „EBA/GL/2019/04“. Pranešimus turėtų teikti asmenys, turintys reikiamus 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).

Dalykas, taikymo sritis ir sąvokų apibrėžtys

Dalykas

5. Šios gairės grindžiamos Direktyvos 2013/36/ES (KRD) 74 straipsnio nuostatomis dėl vidinio valdymo ir įgaliojimais parengti gaires pagal Direktyvos (ES) 2015/2366 (MPD2) 95 straipsnio 3 dalį.

6. Šiose gairėse išdėstomos rizikos valdymo priemonės, kurių finansų įstaigos (kaip apibrėžta toliau 9 punkte) privalo imtis pagal KRD 74 straipsnį siekdamos valdyti savo IRT ir saugumo riziką visose veiklos srityse ir kurių mokėjimo paslaugų teikėjai (MPT, kaip apibrėžta toliau 9 punkte) privalo imtis pagal MPD2 95 straipsnio 1 dalį siekdami valdyti savo operacinę ir saugumo riziką (laikomą IRT ir saugumo rizika), susijusią su jų teikiamomis mokėjimo paslaugomis. Į gaires įtraukti informacijos saugumo, įskaitant kibernetinį saugumą, reikalavimai, susiję su IRT sistemose saugoma informacija.

Taikymo sritis

7. Šios gairės taikomos finansų įstaigoms (kaip apibrėžta 9 punkte) valdant IRT ir saugumo riziką. Šiose gairėse terminas „IRT ir saugumo rizika“ aprėpia su mokėjimo paslaugų teikimu siejamą operacinę ir saugumo riziką pagal MPD2 95 straipsnį.

8. MPT (kaip apibrėžta 9 punkte) atveju šios gairės taikomos jų mokėjimo paslaugų teikimui atsižvelgiant į MPD2 95 straipsnio taikymo sritį ir jame įtvirtintus įgaliojimus. Įstaigų (kaip apibrėžta 9 punkte) atveju šios gairės taikomos visai jų vykdomai veiklai.

Kam skirtos šios gairės?

9. Šios gairės skirtos finansų įstaigoms, kurios šiose gairėse yra 1) MPT, kaip apibrėžta MPD2 4 straipsnio 11 dalyje, ir 2) įstaigos, t. y. kredito įstaigos ir investicinės įmonės, kaip apibrėžta Reglamento (ES) Nr. 575/2013 4 straipsnio 1 dalies 3 punkte. Šios gairės taip pat taikomos Reglamento (ES) Nr. 575/2013 4 straipsnio 1 dalies 40 punkte apibrėžtoms kompetentingoms institucijoms, įskaitant Europos Centrinį Banką, kai šis sprendžia klausimus, susijusius su jam Reglamentu (ES) Nr. 1024/2013 pavestomis užduotimis, ir kompetentingoms institucijoms pagal MPD2, kaip nurodyta Reglamento (ES) Nr. 1093/2010 4 straipsnio 2 dalies i punkte.

Sąvokų apibrėžtys

10. Jei nenurodyta kitaip, Direktyvoje 2013/36/ES (KRD), Reglamente (ES) Nr. 575/2013 (KRR) ir Direktyvoje 2015/2366/ES (MPD2) vartojamos ir apibrėžtos sąvokos šiose gairėse turi tokią pačią reikšmę. Be to, gairėse vartojamos šios sąvokos:

IRT ir saugumo rizika	Rizika patirti nuostolių dėl konfidencialumo pažeidimo, sistemų ir duomenų vientisumo pažeidimo, sistemų ir duomenų netinkamumo ar jų neprieinamumo arba dėl nesugebėjimo per pagrįstą laiką ir patiriant pagrįstas sąnaudas pakeisti informacines technologijas (IT), kai pasikeičia aplinka ar verslo poreikiai (t. y. operatyvumas)[2]. Ji apima saugumo riziką, kylančią dėl netinkamų ar nevykusių vidaus procesų arba išorės įvykių, įskaitant kibernetines atakas arba nepakankamą fizinį saugumą.
Valdymo organas	(a) Kredito įstaigų ir investicinių įmonių atveju šis terminas turi tokią pačią reikšmę, kaip apibrėžta Direktyvos 2013/36/ES 3 straipsnio 1 dalies 7 punkte. (b) Mokėjimo įstaigų ar elektroninių pinigų įstaigų atveju šiuo terminu įvardijami direktoriai arba už mokėjimo įstaigų ir elektroninių pinigų įstaigų valdymą atsakingi asmenys ir tam tikrais atvejais asmenys, atsakingi už mokėjimo įstaigų ir elektroninių pinigų įstaigų mokėjimo paslaugų veiklos valdymą. (c) MPT, nurodytų Direktyvos (ES) 2015/2366 1 straipsnio 1 dalies c, e ir f punktuose, atveju šis terminas turi tokią pačią reikšmę, kaip taikytinuose ES ar nacionalinės teisės aktuose.
Operacinis ar saugumo incidentas	Pavienis įvykis arba tarpusavyje susijusių įvykių grupė, kurių finansų įstaiga neplanavo ir kurie turi arba, tikėtina, turės neigiamą poveikį paslaugų vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui.
Vyresnioji vadovybė	(a) Kredito įstaigų ir investicinių įmonių atveju šis terminas turi tokią pačią reikšmę, kaip apibrėžta Direktyvos 2013/36/ES 3 straipsnio 1 dalies 9 punkte. (b) Mokėjimo įstaigų ir elektroninių pinigų įstaigų atveju šiuo terminu įvardijami fiziniai asmenys, kurie įstaigoje vykdo vykdomąsias funkcijas, atsako už kasdienį įstaigos valdymą ir yra atskaitingi valdymo organui. (c) MPT, nurodytų Direktyvos (ES) 2015/2366 1 straipsnio 1 dalies c, e ir f punktuose, atveju šis terminas turi tokią pačią reikšmę, kaip taikytinuose ES ar nacionalinės teisės aktuose.
Rizikos apetitas	Bendrasis rizikos, kurią siekdami savo strateginių tikslų MPT ir įstaigos nori prisiimti, lygis ir rūšys, atsižvelgiant į jų pajėgumą prisiimti riziką ir verslo modelį.
Audito funkcija	(a) Kredito įstaigų ir investicinių įmonių atveju audito funkcija – tai audito funkcija, kaip nurodyta EBI vidaus valdymo gairių (EBA/GL/2017/11) 22 skirsnyje

[2] Apibrėžtis, pateikta 2014 m. gruodžio 19 d. EBI gairėse dėl bendros priežiūrinio tikrinimo ir vertinimo proceso tvarkos ir metodikos (EBA/GL/2014/13), iš dalies pakeistose EBA/GL/2018/03.

(b) MPT, kurie nėra kredito įstaigos, atveju audito funkcija turi būti nepriklausoma MPT įstaigos viduje arba nuo jos ir gali būti vidaus ir (arba) išorės audito funkcija.

IRT projektai	Bet koks projektas (arba jo dalis), kurį vykdant keičiamos, pakeičiamos, pašalinamos arba įgyvendinamos IRT sistemos ir paslaugos. IRT projektai gali būti didesnių IRT ar verslo transformavimo programų dalis.
Trečioji šalis	Organizacija, su tam tikru subjektu užmezgusi verslo santykius ar sudariusi sutartis dėl produkto ar paslaugos teikimo[3].
Informaciniai ištekliai	Materialūs ar nematerialūs informacijos rinkiniai, kuriuos verta apsaugoti.
IRT turtas	Programinė arba aparatinė įranga, naudojama verslo aplinkoje.
IRT sistemos[4]	IRT, įdiegtos kaip mechanizmo arba tarpusavyje susijusio tinklo, kuriuo remiamos finansų įstaigos operacijos, dalis.
IRT paslaugos[5]	IRT sistemomis vienam ar keliems vidaus arba išorės naudotojams teikiamos paslaugos. Prie jų priskiriamos, pvz., duomenų įvedimo, saugojimo, apdorojimo ir ataskaitų teikimo paslaugos, taip pat stebėsenos, verslo paramos ir pagalbinės sprendimų priėmimo paslaugos.

Įgyvendinimas

Taikymo data

11. Šios gairės taikomos nuo 2020 m. birželio 30 d.

Panaikinimas

12. 2017 m. paskelbtos gairės dėl saugumo priemonių, susijusių su operacine ir saugumo rizika (EBA/GL/2017/17), bus panaikintos šiomis gairėmis nuo šių gairių taikymo datos.

[3] G7 pagrindinėse gairėse dėl trečiųjų šalių kibernetinės rizikos valdymo finansų sektoriuje pateikta apibrėžtis.
[4] Gairėse dėl IRT rizikos vertinimo per priežiūrinio tikrinimo ir vertinimo procesą (SREP) (EBA/GL/ 2017/05) pateikta apibrėžtis.
[5] Ten pat.

IRT ir saugumo rizikos valdymo gairės

1.1. Proporcingumas

1. Visos finansų įstaigos turėtų laikytis šių gairių nuostatų taip, kad tai būtų proporcinga finansų įstaigos dydžiui, vidiniam organizavimui bei finansų įstaigų teikiamų paslaugų ir tiekiamų arba numatomų teikti produktų pobūdžiui, taikymo sričiai, sudėtingumui ir rizikingumui ir kad į visa tai būtų atsižvelgiama.

1.2. Valdymas ir strategija

1.2.1. Valdymas

2. Valdymo organas turėtų užtikrinti, kad IRT ir saugumo rizikai valdyti finansų įstaigos turėtų tinkamą vidaus valdymo ir vidaus kontrolės sistemą. Valdymo organas turėtų nustatyti aiškias funkcijas ir pareigas, susijusias su IRT užduotimis, informacijos saugumo rizikos valdymu ir veiklos tęstinumu, įskaitant valdymo organo ir jo komitetų funkcijas ir pareigas.
3. Valdymo organas turėtų užtikrinti, kad finansų įstaigų darbuotojų skaičius ir įgūdžiai nuolat atitiktų jų IRT operacinius poreikius bei IRT ir saugumo rizikos valdymo procesus ir būtų pakankami, kad būtų užtikrintas IRT strategijos įgyvendinimas. Valdymo organas turėtų užtikrinti, kad būtų paskirtas pakankamas biudžetas pirmiau nurodytiems tikslams įgyvendinti. Be to, finansų įstaigos turėtų užtikrinti, kad visi darbuotojai, įskaitant pagrindines užduotis atliekančius asmenis, būtų kasmet arba prireikus dažniau tinkamai apmokomi IRT ir saugumo rizikos srityje, įskaitant informacijos saugumo klausimus (taip pat žr. 1.4.7 skirsnį).
4. Valdymo organas apskritai atsako už finansų įstaigų IRT strategijos, kuri yra bendros verslo strategijos dalis, parengimą, patvirtinimą ir įgyvendinimo priežiūrą bei už veiksmingos IRT ir saugumo rizikos valdymo sistemos sukūrimą.

1.2.2. Strategija

5. IRT strategija turėtų būti suderinta su finansų įstaigų bendra verslo strategija; joje turėtų būti apibrėžta:
    a) kaip turėtų būti plėtojamos finansų įstaigų IRT siekiant veiksmingai remti jų verslo strategiją ir joje dalyvauti, įskaitant organizacinės struktūros raidą, IRT sistemos pokyčius ir pagrindinius priklausomybės nuo trečiųjų šalių ryšius;
    b) numatoma strategija ir IRT architektūros raida, įskaitant priklausomybės nuo trečiųjų šalių ryšius;
    c) aiškūs informacijos saugumo tikslai, sutelkiant dėmesį į IRT sistemas ir IRT paslaugas, darbuotojus ir procesus.
6. Finansų įstaigos turėtų parengti veiksmų planų rinkinius, į kuriuos įtraukiamos priemonės, kurių imamasi siekiant įgyvendinti IRT strategijos tikslus. Apie juos reikėtų pranešti visiems

susijusiems darbuotojams (įskaitant, kai taikytina ir svarbu, rangovus ir trečiųjų šalių tiekėjus). Veiksmų planus reikėtų reguliariai peržiūrėti siekiant užtikrinti jų aktualumą ir tinkamumą. Finansų įstaigos taip pat turėtų sukurti savo IRT strategijos veiksmingumo ir įgyvendinimo stebėsenos ir vertinimo procesus.

1.2.3. Trečiųjų šalių tiekėjų pasitelkimas

7. Nepažeidžiant EBI gairių dėl užsakomųjų paslaugų (EBA/GL/2019/02) ir MPD2 19 straipsnio, finansų įstaigos turėtų užtikrinti rizikos mažinimo priemonių veiksmingumą, kaip numatyta jų rizikos valdymo sistemoje, įskaitant šiose gairėse nustatytas priemones, kai operacinės mokėjimo paslaugų ir (arba) IRT paslaugų ir bet kurios veiklos rūšies IRT sistemų funkcijos užsakomos, be kita ko, iš grupės subjektų, arba kai pasitelkiamos trečiosios šalys.

8. Siekdamos užtikrinti IRT paslaugų ir IRT sistemų tęstinumą finansų įstaigos turėtų užtikrinti, kad į su tiekėjais (užsakomųjų paslaugų teikėjais, grupės subjektais arba trečiųjų šalių tiekėjais) sudarytose sutartyse ir susitarimuose dėl paslaugų lygio (ir įprastomis aplinkybėmis, ir sutrikus paslaugų teikimui (taip pat žr. 1.7.2 skirsnį)) būtų numatyta:

    a) tinkami ir proporcingi su informacijos saugumu susiję tikslai ir priemonės, įskaitant reikalavimus, kaip antai minimaliuosius kibernetinio saugumo reikalavimus, specifikacijas dėl finansų įstaigos duomenų gyvavimo ciklo, visus reikalavimus dėl duomenų šifravimo, tinklo saugumo ir saugumo stebėsenos procesų ir duomenų centrų buvimo vietos;
    b) operacinių ir saugumo incidentų valdymo procedūros, įskaitant problemų sprendimo ir informavimo procedūras.

9. Finansų įstaigos turėtų vykdyti stebėseną ir siekti užtikrinti, kad tie paslaugų teikėjai laikytųsi nustatytų finansų įstaigos saugumo tikslų, priemonių ir veiklos rezultatų tikslų.

1.3. IRT ir saugumo rizikos valdymo sistema

1.3.1. Organizacija ir tikslai

10. Finansų įstaigos turėtų nustatyti ir valdyti savo IRT ir saugumo riziką. IRT funkcija(-os), apimanti atsakomybę už IRT sistemas, procesus ir saugumo operacijas, turėtų numatyti ir tinkamų procesų ir kontrolės priemonių įdiegimą siekiant užtikrinti, kad visų rūšių rizika būtų nustatoma, analizuojama, matuojama, stebima ir valdoma, kad apie ją būtų pranešama ir kad ji neviršytų finansų įstaigos rizikos apetito ribų, taip pat kad rengiami projektai ir sistemos ir vykdoma veikla atitiktų išorės ir vidaus reikalavimus.

11. Finansų įstaigos turėtų priskirti atsakomybę už IRT ir saugumo rizikos valdymą ir priežiūrą kontrolės funkcijai, laikantis EBI vidaus valdymo gairių (EBA/GL/2017/11) 19 skirsnio reikalavimų. Finansų įstaigos turėtų užtikrinti tokios kontrolės funkcijos nepriklausomumą ir objektyvumą tinkamai atskiriant ją nuo IRT operacijų procesų. Tokia kontrolės funkcija turėtų būti tiesiogiai atskaitinga valdymo organui ir atsakinga už IRT ir saugumo rizikos valdymo sistemos laikymosi stebėseną ir kontrolę. Ji turėtų užtikrinti, kad IRT ir saugumo rizika būtų

nustatoma, matuojama, vertinama, valdoma ir stebima ir kad apie ją būtų pranešama. Finansų įstaigos turėtų užtikrinti, kad tokia kontrolės funkcija neapimtų atsakomybės už vidaus auditą.

Taikydamas rizika pagrįstą metodą vidaus audito funkcijos vykdytojas turėtų gebėti nepriklausomai peržiūrėti ir objektyviai įvertinti visų su IRT ir saugumu susijusių veiksmų atitiktį ir finansų įstaigos padalinių finansų įstaigos politikos ir procedūrų ir išorės reikalavimų laikymąsi, kaip reikalaujama EBI vidaus valdymo gairių (EBA/GL/2017/11) 22 skirsnyje.

12. Kad IRT ir saugumo rizikos valdymo sistema būtų veiksminga, finansų įstaigos turėtų apibrėžti ir priskirti pagrindines funkcijas ir pareigas bei nustatyti atitinkamas atskaitomybės linijas. Tokia sistema turėtų būti visiškai integruota į bendrus finansų įstaigos rizikos valdymo procesus ir su jais suderinta.

13. IRT ir saugumo rizikos valdymo sistemoje turėtų būti įdiegti procesai, kuriuos įgyvendinant būtų galima:

    a) nustatyti IRT ir saugumo rizikos apetitą atsižvelgiant į finansų įstaigos rizikos apetitą;
    b) nustatyti ir įvertinti finansų įstaigai kylančią IRT ir saugumo riziką;
    c) nustatyti IRT ir saugumo rizikos mažinimo priemones, įskaitant kontrolės priemones;
    d) stebėti tų priemonių veiksmingumą ir incidentų, apie kuriuos pranešama, skaičių, MPT atveju įskaitant incidentus, apie kuriuos pranešama pagal MPD2 96 straipsnį ir kurie daro poveikį su IRT susijusiai veiklai, ir prireikus imtis veiksmų siekiant pakoreguoti priemones;
    e) pranešti valdymo organui apie IRT ir saugumo riziką ir kontrolės priemones;
    f) nustatyti ir įvertinti, ar dėl svarbių IRT sistemos arba IRT paslaugų, procesų ar procedūrų pakeitimų ir (arba) po kokio nors svarbaus operacinio ar saugumo incidento kyla kokia nors IRT ir saugumo rizika.

14. Finansų įstaigos turėtų užtikrinti, kad IRT ir saugumo rizikos valdymo sistema būtų užregistruota dokumentuose ir nuolat atnaujinama remiantis patirtimi ją įgyvendinant ir vykdant jos stebėseną. Valdymo organas turėtų bent kartą per metus tvirtinti ir peržiūrėti IRT ir saugumo rizikos valdymo sistemą.

1.3.2. Funkcijų, procesų ir išteklių nustatymas

15. Siekdamos nustatyti kiekvieno su IRT ir saugumo rizika susijusio tarpusavio priklausomybės ryšio svarbą finansų įstaigos turėtų nustatyti, parengti ir palaikyti atnaujintą savo veiklos funkcijų, funkcijų ir pagalbinių procesų apžvalgą.

16. Be to, finansų įstaigos turėtų nustatyti, parengti ir palaikyti atnaujintą informacinių išteklių, kuriais grindžiamos jų verslo funkcijos ir pagalbiniai procesai, kaip antai IRT sistemos, darbuotojai, rangovai, trečiosios šalys ir priklausomybė nuo kitų vidaus ir išorės sistemų ir procesų, apžvalgą, kad galėtų valdyti bent informacinius išteklius, kuriais grindžiamos kritinės veiklos funkcijos ir procesai.

1.3.3. Klasifikavimas ir rizikos vertinimas

17. Finansų įstaigos turėtų klasifikuoti 15 ir 16 punktuose nustatytas veiklos funkcijas, pagalbinius procesus ir informacinius išteklius pagal jų svarbą.

18. Siekdamos apibūdinti tokių nustatytų veiklos funkcijų, pagalbinių procesų ir informacinių išteklių svarbą, finansų įstaigos turėtų atsižvelgti bent į konfidencialumo, vientisumo ir prieinamumo reikalavimus. Turėtų būti aiškiai priskirta atskaitomybė ir atsakomybė už informacinius išteklius.

19. Atlikdamos rizikos vertinimą finansų įstaigos turėtų peržiūrėti informacinių išteklių klasifikavimo tinkamumą ir atitinkamus dokumentus.

20. Finansų įstaigos turėtų nustatyti IRT ir saugumo riziką, darančią poveikį nustatytoms ir pagal svarbą klasifikuotoms veiklos funkcijoms, pagalbiniams procesams ir informaciniams ištekliams. Toks rizikos vertinimas turėtų būti atliekamas ir dokumentuojamas kartą per metus arba prireikus dažniau. Tokį rizikos vertinimą taip pat reikėtų atlikti iš esmės pasikeitus infrastruktūrai, procesams ar procedūroms, darančioms poveikį veiklos funkcijoms, pagalbiniams procesams arba informaciniams ištekliams; po to reikėtų atitinkamai atnaujinti galiojantį finansų įstaigų rizikos vertinimą.

21. Finansų įstaigos turėtų užtikrinti, kad būtų nuolat vykdoma grėsmių ir pažeidžiamumo stebėsena, susijusi su jų veiklos procesais, pagalbinėmis funkcijomis ir informaciniais ištekliais, ir turėtų reguliariai peržiūrėti poveikį jiems darančius rizikos scenarijus.

1.3.4. Rizikos mažinimas

22. Remdamosi rizikos vertinimu finansų įstaigos turėtų nustatyti, kokių priemonių reikia imtis siekiant sumažinti nustatytą IRT ir saugumo riziką iki priimtino lygio ir ar dabartinius veiklos procesus, kontrolės priemones, IRT sistemas ir IRT paslaugas reikia pakeisti. Finansų įstaiga turėtų apsvarstyti, kiek laiko reikia tokiems pokyčiams įgyvendinti, ir kiek laiko reikia, kad būtų imtasi tinkamų rizikos mažinimo priemonių siekiant kuo labiau sumažinti IRT ir saugumo riziką neviršijant finansų įstaigos IRT ir saugumo rizikos apetito.

23. Finansų įstaigos turėtų apibrėžti ir įgyvendinti nustatytos IRT ir saugumo rizikos mažinimo ir informacinių išteklių apsaugos priemones atsižvelgiant į klasifikavimą.

1.3.5. Informavimas

24. Finansų įstaigos turėtų aiškiai ir laiku pateikti rizikos vertinimo rezultatus valdymo organui. Toks informacijos teikimas vyksta nepažeidžiant MPT prievolės teikti kompetentingoms institucijoms atnaujintą ir išsamų rizikos vertinimą, kaip nustatyta Direktyvos (ES) 2015/2366 95 straipsnio 2 dalyje.

1.3.6. Auditas

25. Finansų įstaigos valdymą, sistemas ir procesus, susijusius su jos IRT ir saugumo rizika, turėtų reguliariai tikrinti pakankamai žinių, įgūdžių ir patirties IRT ir saugumo rizikos ir mokėjimų (MPT atveju) srityje turintys auditoriai, kurie galėtų nepriklausomai patikinti valdymo organą jų veiksmingumu. Auditoriai turėtų būti nepriklausomi finansų įstaigos vidaus ar išorės lygmeniu. Tokių auditų dažnis ir sritis turėtų būtų proporcingi atitinkamai IRT ir saugumo rizikai.

26. Finansų įstaigos valdymo organas turėtų patvirtinti audito planą, įskaitant IRT auditą ir svarbius pakeitimus. Audito plane ir jį įgyvendinant, įskaitant audito dažnį, turėtų būti perteikta finansų įstaigai būdinga IRT ir saugumo rizika ir jis turėtų būti jai proporcingas ir reguliariai atnaujinamas.

27. Reikėtų sukurti oficialų tolesnių veiksmų procesą, įskaitant nuostatas dėl kritinių IRT audito rezultatų patikrinimo ir ištaisymo laiku.

1.4. Informacijos saugumas

1.4.1. Informacijos saugumo politika

28. Finansų įstaigos turėtų parengti ir užregistruoti dokumentuose informacijos saugumo politiką, kurioje turėtų būti nustatyti bendro pobūdžio principai ir taisyklės, skirtos apsaugoti finansų įstaigų ir jų klientų duomenų ir informacijos konfidencialumą, vientisumą ir prieinamumą. MPT atveju tokia politika išdėstoma saugumo politikos dokumente, kuris yra patvirtinamas pagal Direktyvos (ES) 2015/2366 5 straipsnio 1 dalies j punktą. Informacijos saugumo politika turėtų atitikti finansų įstaigos informacijos saugumo tikslus ir būti grindžiama atitinkamais rizikos vertinimo proceso rezultatais. Tokią politiką turėtų patvirtinti valdymo organas.

29. Į politiką reikėtų įtraukti pagrindinių informacijos saugumo valdymo srities funkcijų ir pareigų aprašymą; joje reikėtų nustatyti reikalavimus darbuotojams ir rangovams ir su informacijos saugumu susijusius procesus ir technologijas, pažymint, kad už finansų įstaigų informacijos saugumą atsako visų lygmenų darbuotojai ir rangovai. Politika turėtų padėti užtikrinti svarbiausių finansų įstaigos loginių ir fizinių turto objektų, išteklių ir saugomų, perduodamų ar naudojamų neskelbtinų duomenų konfidencialumą, vientisumą ir prieinamumą. Informacijos saugumo politika turėtų būti pateikta visiems finansų įstaigos darbuotojams ir rangovams.

30. Remdamosi informacijos saugumo politika finansų įstaigos turėtų sukurti ir įgyvendinti saugumo priemones, kuriomis būtų mažinama joms kylanti IRT ir saugumo rizika. Tokios priemonės turėtų apimti:

    a) organizavimą ir valdymą pagal 10 ir 11 punktus;
    b) loginį saugumą (1.4.2 skirsnis);
    c) fizinį saugumą (1.4.3 skirsnis);
    d) IRT operacijų saugumą (1.4.4 skirsnis);
    e) saugumo stebėseną (1.4.5 skirsnis);
    f) informacijos saugumo peržiūras, vertinimą ir bandymus (1.4.6 skirsnis);
    g) informacijos saugumo srities mokymą ir informuotumo didinimą (1.4.7 skirsnis).

1.4.2. Loginis saugumas

31. Finansų įstaigos turėtų apibrėžti, dokumentuoti ir įgyvendinti loginės prieigos kontrolės (tapatybės ir prieigos valdymo) procedūras. Tokios procedūros turėtų būti įgyvendinamos, kontroliuojamos, stebimos ir reguliariai peržiūrimos. Procedūros taip pat turėtų apimti anomalijų stebėsenos kontrolės priemones. Tokiose procedūrose turėtų būti įgyvendinti bent toliau išvardyti elementai (terminas „vartotojas“ apima ir techninius vartotojus):

    (a) **būtinybė žinoti, mažiausios privilegijos ir pareigų atskyrimas:** finansų įstaigos turėtų valdyti prieigos prie informacinių išteklių ir jų sistemų teises remdamosi principu „būtina žinoti“, taip pat nuotolinės prieigos atveju. Vartotojams turėtų būti suteikiamos minimalios prieigos teisės, reikalingos jų būtinoms pareigoms įvykdyti („mažiausios privilegijos“ principas), t. y. siekiant užkirsti kelią nepagrįstai prieigai prie didelio duomenų kiekio arba prieigos teisių derinių paskirstymui, kuriuo gali būti naudojamasi siekiant išvengti kontrolės priemonių („pareigų atskyrimo“ principas);

    (b) **vartotojų atskaitomybė:** finansų įstaigos turėtų kuo labiau riboti bendrų ir pasidalijamų vartotojų paskyrų naudojimą ir užtikrinti, kad IRT sistemose atliekant veiksmus būtų galima nustatyti vartotojų tapatybę;

    (c) **privilegijuotos prieigos teisės:** finansų įstaigos turėtų įgyvendinti griežtas privilegijuotos prieigos prie sistemos kontrolės priemones griežtai ribodamos ir įdėmiai stebėdamos padidintas prieigos prie sistemos teises turinčias paskyras (pvz., administratorių paskyras). Siekiant užtikrinti saugų ryšį ir sumažinti riziką, nuotolinę administracinę prieigą prie svarbiausių IRT sistemų reikėtų suteikti tik pagal principą „būtina žinoti“ ir naudojant patikimus autentiškumo patvirtinimo sprendimus;

    (d) **vartotojo veiksmų įrašymas į žurnalą:** į žurnalą turėtų būti įrašomi ir stebimi bent visi privilegijuotų vartotojų veiksmai. Siekiant užkirsti kelią nesankcionuotam duomenų pakeitimui arba ištrynimui prieigos registracijos žurnalus reikėtų saugoti tiek, kiek proporcinga atsižvelgiant į nustatytų veiklos funkcijų, pagalbinių procesų ir informacinių išteklių svarbą, kaip numatyta 1.3.3 skirsnyje, nepažeidžiant ES ir nacionalinės teisės aktuose nustatytų informacijos saugojimo reikalavimų. Finansų įstaiga turėtų naudoti šią informaciją siekdama palengvinti anomalios veiklos, pastebėtos teikiant paslaugas, nustatymą ir tyrimą;

    (e) **prieigos valdymas:** prieigos teises reikėtų suteikti, atšaukti arba keisti laiku, remiantis iš anksto nustatytais patvirtinimo darbo procesais, kuriuose dalyvauja informacijos, prie kurios prieinama, verslo savininkas (informacinių išteklių savininkas). Nutraukus darbo santykius prieigos teisės turėtų būti greitai panaikinamos;

    (f) **pakartotinis prieigos sertifikavimas:** prieigos teises reikėtų reguliariai peržiūrėti siekiant užtikrinti, kad vartotojai neturėtų pernelyg didelių privilegijų ir kad prieigos teisės būtų panaikinamos, kai jų nebereikia;

    (g) **autentiškumo patvirtinimo būdai:** finansų įstaigos turėtų naudoti autentiškumo patvirtinimo būdus, kurie būtų pakankamai patikimi, kad būtų galima tinkamai ir veiksmingai užtikrinti prieigos kontrolės politikos ir procedūrų laikymąsi. Autentiškumo patvirtinimo būdai turi atitikti IRT sistemų, informacijos ar proceso, prie kurio prieinama, svarbą. Tai turėtų būti bent sudėtingi slaptažodžiai arba patikimesni autentiškumo

patvirtinimo būdai (kaip antai dviejų pakopų autentiškumo patvirtinimas) atsižvelgiant į atitinkamą riziką.

32. Elektroninė taikomųjų programų prieiga prie duomenų ir IRT sistemų turėtų būti kuo labiau ribojama ir suteikiama tik kai tai būtina tam tikrai paslaugai teikti.

1.4.3. Fizinis saugumas

33. Siekiant apsaugos finansų įstaigų patalpas, duomenų centrus ir jautrias zonas nuo nesankcionuotos prieigos ir aplinkos pavojų turėtų būti apibrėžtos, užregistruotos dokumentuose ir įgyvendinamos finansų įstaigų fizinio saugumo priemonės.

34. Fizinė prieiga prie IRT sistemų turėtų būti leidžiama tik įgaliotiems asmenims. Įgaliojimai turėtų būti suteikiami atsižvelgiant į asmens užduotis ir atsakomybės sritis ir tik asmenims, kurie yra tinkamai apmokyti ir prižiūrimi. Siekiant užtikrinti, kad nereikalingos prieigos teisės būtų greitai panaikinamos, fizinę prieigą reikėtų reguliariai peržiūrėti.

35. Tinkamos apsaugos nuo aplinkos pavojų priemonės turėtų atitikti pastatų svarbą ir tuose pastatuose vykdomų operacijų ar esančių IRT sistemų svarbą.

1.4.4. IRT operacijų saugumas

36. Finansų įstaigos turėtų įgyvendinti procedūras siekdamos užkirsti kelią IRT sistemų ir IRT paslaugų saugumo problemoms ir turėtų kuo labiau sumažinti jų poveikį IRT paslaugų teikimui. Šios procedūros turėtų apimti:

    a) galimų pažeidžiamumų, kuriuos reikėtų įvertinti ir ištaisyti, nustatymą užtikrinant savalaikį programinės ir aparatinės įrangos atnaujinimą, įskaitant programinę įrangą, kurią finansų įstaigos tiekia savo vidaus ir išorės vartotojams, diegiant kritinius saugumo atnaujinimus arba kompensuojamąsias kontrolės priemones;
    b) saugios visų tinklo komponentų bazinės konfigūracijos įgyvendinimą;
    c) tinklo suskirstymą į segmentus, duomenų praradimo prevencijos sistemas ir tinklo srauto šifravimą (atsižvelgiant į duomenų klasifikaciją);
    d) galinių įrenginių, įskaitant serverius, kompiuterizuotas darbo vietas ir mobiliuosius prietaisus, apsaugos įgyvendinimą; prieš suteikdamos galiniams įrenginiams prieigą prie įstaigos tinklo finansų įstaigos turėtų įvertinti, ar jie atitinka nustatytus saugumo standartus;
    e) užtikrinimą, kad būtų įdiegti programinės įrangos, aparatinės įrangos ir duomenų vientisumo patikrinimo mechanizmai;
    f) saugomų ir perduodamų duomenų šifravimą (atsižvelgiant į duomenų klasifikaciją).

37. Be to, finansų įstaigos turėtų nuolat vertinti, ar dabartinės veiklos aplinkos pokyčiai turi įtakos įgyvendinamoms saugumo priemonėms arba ar reikia priimti papildomas priemones siekiant tinkamai mažinti susijusią riziką. Tokie pakeitimai turėtų būti įtraukti į oficialų finansų įstaigų pokyčių valdymo procesą, kuriuo turėtų būti užtikrinama, kad pakeitimai būtų tinkamai planuojami, bandomi, užregistruojami dokumentuose, patvirtinami ir taikomi.

1.4.5. Saugumo stebėsena

38. Finansų įstaigos turėtų parengti ir įgyvendinti politiką ir procedūras, skirtas nustatyti neįprastus veiksmus, kurie gali daryti poveikį finansų įstaigų informacijos saugumui, ir tinkamai reaguoti į tokius įvykius. Vykdydamos tokią nuolatinę stebėseną, finansų įstaigos turėtų įsidiegti tinkamas ir veiksmingas fizinio ir loginio įsibrovimo ir informacinių išteklių konfidencialumo, vientisumo ir prieinamumo pažeidimų nustatymo ir pranešimo apie juos priemones. Nuolatinės stebėsenos ir nustatymo procesai turėtų apimti:

    a) svarbius vidaus ir išorės veiksnius, įskaitant veiklos ir IRT administracines funkcijas;
    b) operacijas, skirtas nustatyti netinkamos trečiųjų šalių arba kitų subjektų prieigos ir netinkamos vidaus prieigos atvejus;
    c) galimas vidaus ir išorės grėsmes.

39. Finansų įstaigos turėtų sukurti ir įgyvendinti procesus ir organizacines struktūras, kuriomis siekiama nustatyti ir nuolat stebėti saugumo grėsmes, kurios galėtų daryti reikšmingą poveikį jų gebėjimams teikti paslaugas. Finansų įstaigos turėtų aktyviai stebėti technologinę plėtrą siekdamos užtikrinti, kad būtų informuotos apie saugumo riziką. Finansų įstaigos turėtų įgyvendinti nustatymo priemones, pavyzdžiui, kad galėtų nustatyti galimą informacijos nutekėjimą, kenkėjišką kodą ir kitas saugumo grėsmes, taip pat viešai žinomus programinės ir aparatinės įrangos pažeidžiamumus, ir turėtų tikrinti, ar yra susijusių naujų saugumo atnaujinimų.

40. Saugumo stebėsenos procesas taip pat turėtų padėti finansų įstaigai suprasti operacinių ar saugumo incidentų pobūdį, nustatyti tendencijas ir atlikti organizacijos tyrimus.

1.4.6. Informacijos saugumo peržiūros, vertinimas ir testavimai

41. Finansų įstaigos turėtų atlikti įvairias informacijos saugumo peržiūras, vertinimus ir testavimus siekdamos užtikrinti veiksmingą IRT sistemų ir IRT paslaugų pažeidžiamumų nustatymą. Pavyzdžiui, finansų įstaigos gali atlikti spragų analizę vadovaudamosi informacijos saugumo standartais, atitikties peržiūromis, vidaus ir išorės informacinių sistemų auditais arba fizinio saugumo peržiūromis. Be to, įstaiga turėtų nagrinėti gerosios praktikos pavyzdžius, kaip antai programinio kodo peržiūras, pažeidžiamumų vertinimus, įsiskverbimų testavimus ir raudonosios komandos pratybas.

42. Finansų įstaigos turėtų sukurti ir įdiegti informacijos saugumo testavimo sistemą, kurioje būtų patvirtinamas jų informacijos saugumo priemonių patikimumas ir veiksmingumas, ir užtikrinti, kad sistemoje būtų nagrinėjamos grėsmės ir pažeidžiamumai, nustatytos grėsmių stebėsenos ir IRT ir saugumo rizikos vertinimo procese.

43. Informacijos saugumo testavimų sistemoje turėtų būti užtikrinama, kad testavimai:

    a) būtų atliekami nepriklausomų testuotojų, turinčių pakankamai žinių, įgūdžių ir patirties testuojant informacijos saugumo priemones ir nedalyvavusių kuriant informacijos saugumo priemones;

b) apimtų pažeidžiamumų skenavimus ir įsiskverbimų testavimus (įskaitant, kai būtina ir tinkama, grėsmėmis grindžiamus įsiskverbimų testavimus), atitinkančius veiklos procesuose ir sistemose nustatytos rizikos lygį.

44. Finansų įstaigos turėtų atlikti einamuosius ir pakartotinius saugumo priemonių testavimus. Visų kritinių IRT sistemų atveju (17 punktas) tokie testavimai turėtų būti atliekami bent kasmet, o MPT atveju jie atliekami vykdant išsamų su teikiamomis mokėjimo paslaugomis susijusios saugumo rizikos vertinimą, kaip numatyta MPD2 95 straipsnio 2 dalyje. Nekritinės sistemos turėtų būti testuojamos reguliariai taikant rizika pagrįstą metodą, bet ne rečiau nei kartą per trejus metus.

45. Finansų įstaigos turėtų užtikrinti, kad saugumo priemonių testavimai būtų atliekami pasikeitus infrastruktūrai, procesams ar procedūroms ir atlikus pakeitimus dėl svarbių operacinių ar saugumo incidentų arba pradėjus naudoti naujas ar iš esmės pakeistas kritines internetines taikomąsias programas.

46. Finansų įstaigos turėtų stebėti ir vertinti saugumo testavimų rezultatus ir atitinkamai atnaujinti savo saugumo priemones ir, kai tai apima svarbiausių IRT sistemų priemones, tai daryti nepagrįstai nedelsiant.

47. MPT atveju testavimo sistemoje taip pat turėtų būti saugumo priemonių, susijusių su 1) mokėjimo terminalais ir prietaisais, naudojamais mokėjimo paslaugoms teikti, 2) mokėjimo terminalais ir prietaisais, naudojamais mokėjimo paslaugų vartotojų (MPV) autentiškumui patvirtinti, ir 3) prietaisais ir programine įranga, kurią MPT teikia MPV autentiškumo patvirtinimo kodams generuoti (gauti).

48. Remiantis pastebėtomis grėsmėmis saugumui ir atsižvelgiant į atliktus pakeitimus, reikėtų atlikti testavimus siekiant įtraukti svarbių ir žinomų potencialių atakų scenarijus.

1.4.7. Mokymas ir informuotumas informacijos saugumo klausimais

49. Finansų įstaigos turėtų parengti visiems darbuotojams ir rangovams skirtą mokymo programą, įskaitant periodinio informuotumo saugumo klausimais didinimo programas, siekdamos užtikrinti jų pasirengimą vykdyti savo pareigas laikantis atitinkamos saugumo politikos ir procedūrų, kad būtų sumažintas žmonių klaidų, vagystės, sukčiavimo, piktnaudžiavimo ar nuostolių atvejų skaičius, ir pašalinti su informacijos saugumu susijusią riziką. Finansų įstaigos turėtų užtikrinti, kad pagal mokymo programą visi darbuotojai ir rangovai būtų mokomi bent kartą per metus.

1.5. IRT operacijų valdymas

50. Finansų įstaigos turėtų valdyti savo IRT operacijas, grindžiamas dokumentuotais ir įgyvendintais procesais ir procedūromis (kurios MPT atveju apima saugumo politikos dokumentus, kaip numatyta MPD2 5 straipsnio 1 dalies j punkte), kurias tvirtina valdymo organas. Tokiame dokumentų rinkinyje reikėtų aprašyti, kaip finansų įstaigos naudoja, stebi ir valdo savo IRT sistemas ir paslaugas, įskaitant kritinių IRT operacijų dokumentavimą, ir finansų įstaigos turėtų turėti galimybę palaikyti aktualų IRT išteklių sąrašą.

51. Finansų įstaigos turėtų užtikrinti, kad jų IRT operacijų vykdymas atitiktų jų verslo reikalavimus. Finansų įstaigos turėtų palaikyti ir, kai įmanoma, didinti savo IRT operacijų veiksmingumą, įskaitant (bet ne tik) poreikį apsvarstyti, kaip kuo labiau sumažinti galimas klaidas, susijusias su rankiniu būdu atliekamų užduočių vykdymu.

52. Finansų įstaigos turėtų įgyvendinti kritinių IRT operacijų įrašymo į žurnalą ir stebėsenos procedūras, kad būtų galima nustatyti, analizuoti ir ištaisyti klaidas.

53. Finansų įstaigos turėtų palaikyti aktualų savo IRT išteklių (įskaitant IRT sistemas, tinklo prietaisus, duomenų bazes ir kt.) sąrašą. IRT išteklių sąraše turėtų būti saugoma IRT išteklių konfigūracija, nuorodos ir įvairių IRT išteklių tarpusavio priklausomybės ryšiai, kad būtų galima užtikrinti tinkamą konfigūravimo ir pokyčių valdymo procesą.

54. IRT išteklių sąrašas turėtų būti pakankamai išsamus, kad būtų galima greitai nustatyti IRT išteklių, jo buvimo vietą, saugumo klasifikaciją ir savininką. Išteklių tarpusavio priklausomybės ryšiai turėtų būti dokumentuojami, kad būtų galima reaguoti į saugumo ir operacinius incidentus, įskaitant kibernetines atakas.

55. Finansų įstaigos turėtų stebėti ir valdyti IRT išteklių gyvavimo ciklus siekdamos užtikrinti, kad jie ir toliau atitiktų verslo ir rizikos valdymo reikalavimus ir su jais derėtų. Finansų įstaigos turėtų stebėti, ar jų išorės ar vidaus tiekėjai ir kūrėjai palaiko jų IRT išteklius ir ar remiantis dokumentuotais procesais taikomos visos reikiamos tobulinimo ir modernizavimo priemonės. Su pasenusiais ar nepalaikomais IRT ištekliais susijusią riziką reikėtų vertinti ir mažinti.

56. Siekdamos laiku užkirsti kelią svarbioms su IRT sistemomis ir nepakankamais IRT pajėgumais susijusių veiklos rezultatų problemoms, jas nustatyti ir į jas reaguoti, finansų įstaigos turėtų įgyvendinti veiklos rezultatų ir pajėgumų planavimo ir stebėsenos procesus.

57. Finansų įstaigos turėtų sukurti ir įgyvendinti duomenų ir IRT sistemų atsarginio kopijavimo ir atstatymo procedūras, kad prireikus jas būtų galima atkurti. Atsarginio kopijavimo mastą ir dažnį reikėtų nustatyti remiantis veiklos atkūrimo reikalavimais ir atsižvelgiant į duomenų ir IRT sistemų svarbą ir vertinti atliekant rizikos vertinimą. Reikėtų reguliariai atlikti atsarginio kopijavimo ir atstatymo procedūrų testavimus.

58. Finansų įstaigos turėtų užtikrinti, kad duomenų ir IRT sistemų atsarginės kopijos būtų saugiai saugomos ir būtų laikomos pakankamai toli nuo pagrindinės buvimo vietos, kad joms nekiltų tokia pat rizika.

3.5.1 IRT incidentų ir problemų valdymas

59. Finansų įstaigos turėtų sukurti ir įgyvendinti incidentų ir problemų valdymo procesą, kurį taikant būtų stebimi ir į žurnalą įrašomi operaciniai ir saugumo IRT incidentai, o finansų įstaigos sutrikimų atveju galėtų tęsti arba laiku vėl pradėti vykdyti svarbiausias veiklos funkcijas ir procesus. Finansų įstaigos turėtų nustatyti tinkamus kriterijus ir ribines vertes, kuriomis remiantis įvykius būtų galima pripažinti operaciniais ar saugumo incidentais, kaip apibrėžta šių gairių skirsnyje „Sąvokų apibrėžtys“, ir ankstyvojo perspėjimo rodiklius, kurie turėtų būti įspėjimas, kad būtų galima anksti nustatyti tokius incidentus. Tokie kriterijai ir ribinės vertės

MPT atveju nustatomos nepažeidžiant didelių incidentų klasifikavimo, kaip numatyta MPD2 96 straipsnyje ir Gairėse dėl pranešimų apie didelius incidentus pagal MPD2 (EBA/GL/2017/10).

60. Siekdamos kuo labiau sumažinti neigiamų įvykių poveikį ir laiku užtikrinti atkūrimą finansų įstaigos turėtų sukurti tinkamus procesus ir organizacines struktūras, kad būtų užtikrinta nuosekli kompleksinė operacinių ir saugumo incidentų stebėsena, valdymas ir tolesni veiksmai ir kad būtų nustatomos ir pašalinamos pagrindinės priežastys siekiant užkirsti kelią pakartotiniams incidentams. Incidentų ir problemų valdymo procese reikėtų nustatyti:

    a) incidentų nustatymo, sekimo, įrašymo į žurnalą, suskirstymo į kategorijas ir klasifikavimo pagal prioritetus procedūras atsižvelgiant į jų svarbą veiklai;
    b) funkcijas ir pareigas pagal įvairius incidentų scenarijus (pvz., susijusius su klaidomis, triktimis, kibernetinėmis atakomis);
    c) problemų valdymo procedūras, naudojamas siekiant nustatyti, analizuoti ir pašalinti pagrindinę vieno ar kelių incidentų priežastį: finansų įstaiga turėtų analizuoti operacinius ar saugumo incidentus, galinčius padaryti poveikį finansų įstaigai, kurie buvo nustatyti ir (arba) įvyko organizacijos viduje ir (arba) už jos ribų, ir turėtų apsvarstyti pagrindines pamokas, įgytas atlikus šią analizę ir atitinkamai atnaujinti saugumo priemones;
    d) veiksmingus vidaus komunikacijos planus, įskaitant pranešimo apie incidentus ir eskalavimo procedūras, apimančias ir su saugumu susijusius klientų skundus, siekiant užtikrinti, kad:
        i) apie incidentus, galinčius padaryti didelį neigiamą poveikį kritinėms IRT sistemoms ir IRT paslaugoms, būtų pranešama atitinkamai vyresniajai vadovybei ir IRT vyresniajai vadovybei;
        ii) *ad hoc* pagrindu valdymo organui būtų pranešama apie didelius incidentus ir bent jau apie poveikį, reagavimą ir papildomas kontrolės priemones, kurias reikia nustatyti dėl incidentų;
    e) reagavimo į incidentus procedūras siekiant sumažinti su incidentais susijusį poveikį ir užtikrinti, kad paslaugos būtų vėl teikiamos laiku ir saugiai;
    f) konkrečius išorės komunikacijos planus, susijusius su kritinėmis svarbos veiklos funkcijomis ir procesais, siekiant:
        i) bendradarbiauti su atitinkamais suinteresuotaisiais subjektais siekiant veiksmingai reaguoti į incidentą ir po jo atsigauti;
        ii) laiku pateikti reikiamą informaciją išorės šalims (pvz., klientams, kitiems rinkos dalyviams, priežiūros institucijai) laikantis taikytinų normų.

1.6. IRT projektų ir pokyčių valdymas

1.6.1. IRT projektų valdymas

61. Finansų įstaiga turėtų įgyvendinti programą ir (arba) projektų valdymo procesą, kuriame būtų apibrėžtos funkcijos, pareigos ir atsakomybės sritys, siekiant veiksmingai paremti IRT strategijos įgyvendinimą.

62. Finansų įstaiga turėtų tinkamai stebėti ir mažinti IRT projektų portfelyje kylančią riziką (programų valdymas) kartu atsižvelgdama į riziką, kuri gali kilti dėl įvairių projektų tarpusavio priklausomybės ryšių ir daugelio projektų priklausomybės nuo tų pačių išteklių ir (arba) ekspertų.

63. Finansų įstaiga turėtų parengti ir įgyvendinti IRT projektų valdymo politiką, kurioje būtų nustatyta bent:

    a) projekto tikslai;
    b) funkcijos ir pareigos;
    c) projekto rizikos vertinimas;
    d) projekto planas, trukmė ir veiksmai;
    e) pagrindiniai etapai;
    f) pokyčių valdymo reikalavimai.

64. IRT projektų valdymo politika reikėtų užtikrinti, kad informacijos saugumo reikalavimus analizuotų ir tvirtintų asmuo, nepriklausomas nuo kūrimo funkciją atliekančio asmens.

65. Finansų įstaiga turėtų užtikrinti, kad projekto grupė aprėptų visas į IRT projektą įtrauktas sritis ir kad projekto grupė turėtų žinių, kurių reikia saugiam ir sėkmingam projekto įgyvendinimui užtikrinti.

66. Apie IRT projektų sukūrimą ir pažangą ir su jais susijusią riziką reikėtų pranešti valdymo organui pateikiant individualius arba apibendrintus duomenis, priklausomai nuo IRT projektų svarbos ir dydžio, reguliariai ir prireikus *ad hoc* pagrindu. Finansų įstaigos turėtų įtraukti projektų riziką į savo rizikos valdymo sistemą.

1.6.2. IRT sistemų įsigijimas ir kūrimas

67. Finansų įstaigos turėtų sukurti ir įgyvendinti IRT sistemų įsigijimo, kūrimo ir palaikymo valdymo procesą. Šis procesas turėtų būti sukurtas remiantis rizika pagrįstu metodu.

68. Finansų įstaiga turėtų užtikrinti, kad prieš įsigyjant ar sukuriant IRT sistemas būtų aiškiai apibrėžti funkciniai ir nefunkciniai reikalavimai (įskaitant informacijos saugumo reikalavimus) ir kad atitinkami vadovai juos patvirtintų.

69. Finansų įstaiga turėtų užtikrinti, kad būtų įgyvendintos priemonės, kuriomis būtų sumažinama nenumatyto IRT sistemų pakeitimo arba tyčinio manipuliavimo jomis jas kuriant ir įgyvendinant gamybos aplinkoje rizika.

70. Finansų įstaigose turėtų būti įgyvendinta IRT sistemų testavimo ir patvirtinimo prieš pradedant jas naudoti metodika. Metodikoje turėtų būti atsižvelgiama į veiklos procesų ir išteklių svarbą. Atliekant testavimus reikėtų užtikrinti, kad naujos IRT sistemos veiktų, kaip numatyta. Taip pat turėtų būti naudojama testavimo aplinka, tinkamai atitinkanti gamybos aplinką.

71. Finansų įstaigos turėtų atlikti IRT sistemų, IRT paslaugų ir informacijos saugumo priemonių testavimus, kad nustatytų galimus saugumo trūkumus, pažeidimus ir incidentus.

72. Finansų įstaiga turėtų įdiegti atskirą IRT aplinką, kad užtikrintų tinkamą pareigų atskyrimą ir sumažintų nepatikrintų pokyčių gamybos sistemoms poveikį. Konkrečiai kalbant, finansų įstaiga

turėtų užtikrinti gamybos aplinkos atskyrimą nuo kūrimo, testavimo ir kitos ne gamybos aplinkos. Finansų įstaiga turėtų užtikrinti gamybos duomenų vientisumą ir konfidencialumą ne gamybos aplinkoje. Prieigą prie gamybos duomenų turi tik leidimus turintys naudotojai.

73. Finansų įstaigos turėtų įgyvendinti įstaigos viduje kuriamų IRT sistemų programinių kodų vientisumo apsaugos priemones. Siekdamos sumažinti nereikalingą priklausomybę nuo konkrečių sričių ekspertų jos taip pat turėtų išsamiai dokumentuoti IRT sistemų kūrimą, įgyvendinimą, veikimą ir (arba) konfigūravimą. IRT sistemų dokumentacija, jei taikytina, turėtų apimti bent vartotojų dokumentaciją, techninių sistemų dokumentaciją ir eksploatacijos procedūras.

74. Finansų įstaigoje įdiegti IRT sistemų įsigijimo ir kūrimo procesai taip pat turėtų būti taikomi IRT sistemoms, kurias taikydami rizika pagrįstą metodą kuria arba valdo IRT organizacijai nepriklausantys galutiniai veiklos funkcijos vartotojai (pvz., apskaitos taikomosios programos, kurias naudoja galutiniai vartotojai). Finansų įstaiga turėtų pildyti tokių taikomųjų programų, palaikančių kritines veiklos funkcijas ar procesus, registrą.

1.6.3. IRT pokyčių valdymas

75. Siekdamos užtikrinti, kad visi IRT sistemų pakeitimai būtų registruojami, testuojami, vertinami, patvirtinami, įdiegiami ir patikrinami užtikrinant kontrolę, finansų įstaigos turėtų sukurti ir įgyvendinti IRT pokyčių valdymo procesą. Finansų įstaigos turėtų tvarkyti pokyčius ekstremaliųjų situacijų atveju (t. y. pokyčius, kuriuos reikia įgyvendinti kuo skubiau) laikydamosi tinkamas apsaugos priemones užtikrinančių procedūrų.

76. Finansų įstaigos turėtų vertinti, ar dabartinės veiklos aplinkos pokyčiai daro įtakos turimoms saugumo priemonėms arba ar reikalauja papildomų susijusios rizikos mažinimo priemonių. Tokie pokyčiai turėtų atitikti finansų įstaigų oficialų pokyčių valdymo procesą.

1.7. Veiklos tęstinumo valdymas

77. Finansų įstaigos turėtų sukurti patikimą veiklos tęstinumo valdymo (VTV) procesą siekiant rimtų veiklos sutrikimų atveju užtikrinti kuo didesnį įstaigos pajėgumą nepertraukiamai vykdyti veiklą ir apriboti nuostolius, kaip numatyta Direktyvos 2013/36/ES 85 straipsnio 2 dalyje ir EBI vidaus valdymo gairių (EBA/GL/2017/11) VI antraštinėje dalyje.

1.7.1. Poveikio veiklai analizė

78. Užtikrindamos patikimą veiklos tęstinumo valdymą finansų įstaigos turėtų atlikti poveikio veiklai analizę (PVA) analizuodamos joms kylančią rimtų veiklos sutrikimų riziką, taip pat kiekybiškai ir kokybiškai vertindamos jų galimą poveikį (be kita ko, konfidencialumui, vientisumui ir prieinamumui), remdamosi vidaus ir (arba) išorės duomenimis (pvz., trečiųjų šalių tiekėjų duomenimis, kurie yra svarbūs veiklos procesui, arba viešai prieinamais duomenimis, kurie gali būti svarbūs PVA) ir scenarijų analize. Atliekant PVA taip pat reikėtų atsižvelgti į nustatytų ir klasifikuotų veiklos funkcijų, pagalbinių procesų, trečiųjų šalių ir

informacinių išteklių svarbą ir jų tarpusavio priklausomybės ryšius, kaip numatyta 1.3.3 skirsnyje.

79. Finansų įstaigos turėtų užtikrinti, kad jų IRT sistemos ir IRT paslaugos būtų sukurtos atsižvelgiant į PVA, pavyzdžiui, numatant tam tikrų kritinių komponentų dubliavimą siekiant užkirsti kelią sutrikimams dėl įvykių, darančių poveikį tiems komponentams.

1.7.2. Veiklos tęstinumo planavimas

80. Remdamosi savo PVA finansų įstaigos turėtų parengti veiklos tęstinumo užtikrinimo planus (veiklos tęstinumo planus, VTP), kurie turėtų būti užregistruoti dokumentuose ir patvirtinti valdymo organų. Planuose turėtų būti konkrečiai nagrinėjama rizika, kuri galėtų padaryti neigiamą poveikį IRT sistemoms ir IRT paslaugoms. Planais turėtų būti remiami tikslai apsaugoti ir, jei būtina, naujai apibrėžti veiklos funkcijų, pagalbinių procesų ir informacinių išteklių konfidencialumą, vientisumą ir prieinamumą. Rengdamos tokius planus finansų įstaigos, kai tinkama, turėtų tai koordinuoti su atitinkamomis vidaus ir išorės suinteresuotosiomis šalimis.

81. Finansų įstaigos turėtų įgyvendinti VTP siekdamos užtikrinti, kad galėtų tinkamai reaguoti į galimų sutrikimų scenarijus ir po sutrikimų vėl pradėti vykdyti savo kritinę veiklą neviršydamos nustatyto atkūrimo termino (t. y. didžiausio laikotarpio, per kurį sistemą ar procesą būtina atkurti po incidento) ir nustatyto atkūrimo momento (t. y. didžiausio laikotarpio, per kurį incidento atveju duomenų praradimas laikomas priimtinu). Rimtai sutrikus veiklai, kai tenka taikyti konkrečius veiklos tęstinumo planus, remdamosi rizika pagrįstu metodu finansų įstaigos turėtų teikti pirmenybę veiklos tęstinumo veiksmams, kurie gali būti grindžiami pagal 1.3.3 skirsnį atliktu rizikos vertinimu. MPT atveju tai, pavyzdžiui, gali būti pagalba toliau tvarkant kritines operacijas, kol dedamos pastangos ištaisyti padėtį.

82. Savo VTP finansų įstaiga turėtų apsvarstyti įvairius scenarijus, įskaitant kraštutinius, bet įmanomus, su kuriais jai gali tekti susidurti, įskaitant kibernetinės atakos scenarijų, ir įvertinti galimą tokių scenarijų poveikį. Remdamasi tokiais scenarijais finansų įstaiga turėtų aprašyti, kaip užtikrinamas IRT sistemų ir paslaugų tęstinumas ir finansų įstaigos informacijos saugumas.

1.7.3. Reagavimo ir atkūrimo planai

83. Remdamosi PVA (78 punktas) ir įmanomais scenarijais (82 punktas) finansų įstaigos turėtų parengti reagavimo ir atkūrimo planus. Tokiuose planuose reikėtų nurodyti, kokiomis sąlygomis planai gali būti taikomi ir kokių veiksmų reikėtų imtis siekiant užtikrinti bent kritinių finansų įstaigose įdiegtų IRT sistemų ir IRT paslaugų prieinamumą, tęstinumą ir atkūrimą. Reagavimo ir atkūrimo planais turėtų būti siekiama įgyvendinti finansų įstaigų operacijų atkūrimo tikslus.

84. Reagavimo ir atkūrimo planuose reikėtų apsvarstyti ir trumpalaikius, ir ilgalaikius atkūrimo variantus. Planai turėtų būti:

    a) parengti daugiausia dėmesio skiriant kritinių veiklos funkcijų, pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių atkūrimui siekiant išvengti neigiamo poveikio finansų įstaigų veikimui ir finansų sistemai, įskaitant mokėjimo

sistemas ir mokėjimo paslaugų vartotojus, taip pat siekiant užtikrinti neįvykdytų mokėjimo operacijų įvykdymą;

b) užregistruoti dokumentuose, kuriais galėtų naudotis veiklos ir veiklą palaikantys skyriai ir kuriuos būtų galima skubiai pritaikyti iškilus nenumatytam atvejui;

c) atnaujinami atsižvelgiant į patirtį, sukauptą įvykus incidentams ir atliekant testavimus, nustatytą riziką ir grėsmes ir pasikeitusius atkūrimo tikslus ir prioritetus.

85. Planuose taip pat turėtų būti vertinamos alternatyvos, kai trumpalaikis atkūrimas gali būti neįmanomas dėl sąnaudų, rizikos, logistikos ar nenumatytų aplinkybių.

86. Be to, reagavimo ir atkūrimo planuose finansų įstaiga turėtų apsvarstyti ir įgyvendinti tęstinumo priemones, kad sumažintų trečiųjų šalių tiekėjų, kurie yra itin svarbūs finansų įstaigos IRT paslaugų tęstinumui, problemas (laikantis EBI gairių dėl užsakomųjų paslaugų (EBA/GL/2019/02) nuostatomis dėl veiklos tęstinumo planų).

1.7.4. Planų testavimai

87. Finansų įstaigos turėtų reguliariai atlikti savo VTP testavimus. Visų pirma, jos turėtų užtikrinti, kad kritinių veiklos funkcijų, pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių (įskaitant, jei taikytina, trečiąsias šalis) VTP būtų testuojami bent kartą per metus, kaip numatyta 89 punkte.

88. VTP reikėtų atnaujinti bent kartą per metus remiantis testavimų rezultatais, surinktais duomenimis apie grėsmes ir su ankstesniais įvykiais susijusia patirtimi. Tam tikrais atvejais taip pat reikėtų apsvarstyti galimybę atnaujinti VTP pasikeitus atkūrimo tikslams (įskaitant nustatytą atkūrimo terminą ir nustatytą atkūrimo momentą) ir (arba) pasikeitus veiklos funkcijoms, pagalbiniams procesams ir informaciniams ištekliams.

89. Atlikdamos savo VTP testavimus finansų įstaigos turėtų įrodyti, kad geba išlaikyti savo veiklos gyvybingumą, kol bus atkurtos kritinės operacijos. Visų pirma, jie turėtų:

a) apimti testavimus pagal pakankamai rimtus, bet įmanomus scenarijus, įskaitant tuos, kurie buvo nagrinėjami rengiant VTP (ir, kai taikytina, atlikti trečiųjų šalių teikiamų paslaugų testavimus); tam kritines veiklos funkcijas, pagalbinius procesus ir informacinius išteklius reikėtų perkelti į atstatymo po krizės aplinką ir įrodyti, kad joje pavyksta vykdyti veiklą per pakankamai reprezentatyvų laikotarpį ir kad po to pavyksta atkurti įprastą veikimą;

b) būti parengti taip, kad būtų kvestionuojamos prielaidos, kuriomis pagrįsti VTP, įskaitant valdymo priemones ir informavimo krizės atveju planus, ir

c) apimti procedūras, kuriomis patikrinamas darbuotojų ir rangovų, IRT sistemų ir IRT paslaugų gebėjimas tinkamai reaguoti į 89 punkto a papunktyje apibrėžtus scenarijus.

90. Testavimų rezultatai turėtų būti dokumentuojami; visus per testavimus nustatytus trūkumus reikėtų išnagrinėti ir pašalinti bei apie juos pranešti valdymo organui.

1.7.5. Ryšiai krizės sąlygomis

91. Sutrikus veiklai arba iškilus nenumatytai situacijai, įgyvendindamos VTP, finansų įstaigos turėtų būti įsidiegusios veiksmingas informavimo krizės atveju priemones, kad visi svarbūs vidaus ir išorės suinteresuotieji subjektai, įskaitant kompetentingas institucijas, kai to reikalaujama pagal nacionalines normas, ir atitinkamus tiekėjus (užsakomųjų paslaugų teikėjus, grupės subjektus arba trečiųjų šalių tiekėjus), būtų laiku ir tinkamai informuoti.

1.8. Ryšių su mokėjimo paslaugų vartotojais vadyba

92. MPT turėtų sukurti ir įgyvendinti procesus, kuriais būtų didinamas MPV informuotumas apie su mokėjimo paslaugomis susijusią saugumo riziką ir MPV būtų teikiama pagalba ir patarimai.

93. MPV teikiamą pagalbą ir patarimus reikėtų atnaujinti atsižvelgiant į naujas grėsmes ir pažeidžiamas vietas, MPV reikėtų informuoti apie pokyčius.

94. Jeigu tai įmanoma pagal produkto funkcionalumą, MPT turėtų leisti MPV išjungti tam tikras mokėjimų funkcijas, susijusias su MPT mokėjimo paslaugų vartotojams teikiamomis mokėjimo paslaugomis.

95. Jeigu pagal Direktyvos (ES) 2015/2366 68 straipsnio 1 dalį MPT susitarė su mokėtoju dėl taikant tam tikras mokėjimo priemones vykdomų mokėjimo operacijų sumų apribojimų, MPT turėtų pasiūlyti mokėtojui galimybę koreguoti tas ribas jas padidinant iki didžiausios sutartos ribos.

96. MPT turėtų pasiūlyti MPV galimybę gauti pranešimus apie bandymus ir (arba) nepavykusius bandymus inicijuoti mokėjimo operacijas, kad jie galėtų nustatyti sukčiavimo ar piktnaudžiavimo jų sąskaita atvejus.

97. MPT turėtų nuolat informuoti MPV apie saugumo procedūrų atnaujinimą, darantį poveikį MPV teikiant mokėjimo paslaugas.

98. MPT turėtų teikti MPV pagalbą visais klausimais ir atsiliepti į pagalbos prašymus ir pranešimus apie anomalijas ar su mokėjimo paslaugų saugumo aspektais susijusias problemas. MPV turėtų būti tinkamai informuojami, kaip gauti tokią pagalbą.