Suvestinė redakcija nuo 2021-08-20 iki 2021-12-31

Nutarimas paskelbtas: TAR 2020-11-26, i. k. 2020-25173

LIETUVOS BANKO VALDYBA

NUTARIMAS DĖL INFORMACINIŲ IR RYŠIŲ TECHNOLOGIJŲ IR SAUGUMO RIZIKOS VALDYMO REIKALAVIMŲ APRAŠO PATVIRTINIMO

2020 m. lapkričio 26 d. Nr. 03-174
Vilnius

Vadovaudamasi Lietuvos Respublikos Lietuvos banko įstatymo 42 straipsnio 4 dalies 1 punktu ir Lietuvos Respublikos mokėjimų įstatymo 56 straipsnio 2 ir 3 dalimis, Lietuvos banko valdyba n u t a r i a :

1. Patvirtinti Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašą (pridedama).
2. Pripažinti netekusiu galios Lietuvos banko valdybos 2018 m. gruodžio 20 d. nutarimą Nr. 03-264 „Dėl Operacinės ir saugumo rizikos valdymo reikalavimų mokėjimo paslaugų teikėjams aprašo patvirtinimo“.
3. Nustatyti, kad šis nutarimas įsigalioja 2021 m. sausio 1 d.

Valdybos pirmininkas Vitas Vasiliauskas

PATVIRTINTA
Lietuvos banko valdybos
2020 m. lapkričio 26 d.
nutarimu Nr. 03-174

INFORMACINIŲ IR RYŠIŲ TECHNOLOGIJŲ IR SAUGUMO RIZIKOS VALDYMO REIKALAVIMŲ APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų apraše (toliau – Aprašas) nustatytos rizikos valdymo priemonės, kurių privalo imtis Aprašo 2 punkte nurodyti finansų rinkos dalyviai, siekdami valdyti informacinių ir ryšių technologijų (IRT) ir saugumo riziką visoje savo veikloje, ir mokėjimo paslaugų teikėjai, siekdami valdyti operacinę ir saugumo riziką, laikomą IRT ir saugumo rizika ir susijusią su jų teikiamomis mokėjimo paslaugomis. Aprašas apima informacijos saugumo, įskaitant kibernetinį saugumą, reikalavimus tokia apimtimi, kiek informacija yra saugoma, apdorojama ir perduodama per IRT sistemas.

2. Aprašo nuostatos taikomos:

2.1. Lietuvos Respublikoje įsteigtiems bankams, elektroninių pinigų įstaigoms, finansų maklerio įmonėms ir šių subjektų, licencijuotų ne Europos Sąjungos valstybėse narėse, filialams, mokėjimo įstaigoms, centrinėms kredito unijoms ir kredito unijoms (toliau – Įstaiga), išskyrus Aprašo 32, 53, 57 punktų ir IX skyriaus nuostatas, kurios taikomos šiems subjektams tuo atveju, jeigu jie yra mokėjimo paslaugų teikėjai (MPT), teikiantys mokėjimo paslaugas pagal Lietuvos Respublikos mokėjimų įstatymą (išskyrus 2.2 papunktyje nurodytus MPT);

2.2. Lietuvos Respublikoje įsteigtiems užsienio bankų, elektroninių pinigų įstaigų, mokėjimo įstaigų, licencijuotų Europos Sąjungos valstybėse narėse, filialams, teikiantiems mokėjimo paslaugas pagal Lietuvos Respublikos mokėjimų įstatymą, – Aprašo IX skyriaus nuostatos.

Punkto pakeitimai:
Nr. 03-123, 2021-08-19, paskelbta TAR 2021-08-19, i. k. 2021-17747

3. Aprašas parengtas atsižvelgiant į 2019 m. lapkričio 29 d. Europos bankininkystės institucijos IRT ir saugumo rizikos valdymo gaires EBA/GL/2019/04.

4. Pagrindinės vartojamos sąvokos:

4.1. **informaciniai ištekliai** – materialieji arba nematerialieji informaciniai rinkiniai, kurie turi būti apsaugoti;

4.2. **IRT ir saugumo rizika** – rizika patirti nuostolių dėl duomenų konfidencialumo pažeidimo, sistemų ir duomenų vientisumo pažeidimo, sistemų ir duomenų netinkamumo ar jų neprieinamumo arba dėl negebėjimo per pagrįstą laiką ir patiriant pagrįstų sąnaudų pakeisti informacines technologijas (IT), kai pasikeičia aplinka ar verslo poreikiai. IRT ir saugumo rizika apima saugumo riziką, kylančią dėl netinkamų ar nevykusių vidaus procesų arba išorės įvykių, įskaitant kibernetines atakas arba nepakankamą fizinį saugumą;

4.3. **IRT paslaugos** – vienam ar keliems vidaus arba išorės IRT sistemų vartotojams teikiamos paslaugos. Prie jų priskiriamos, pvz., duomenų įvedimo, saugojimo, apdorojimo ir ataskaitų teikimo paslaugos, taip pat stebėsenos, verslo paramos ir pagalbinės sprendimų priėmimo paslaugos;

4.4. **IRT projektas** – bet koks projektas (arba jo dalis), kurį vykdant keičiamos, pašalinamos arba įgyvendinamos IRT sistemos ir paslaugos. IRT projektai gali būti didesnių IRT ar verslo keitimo programų dalis;

4.5. **IRT sistemos** – IRT, įdiegtos kaip mechanizmo arba tarpusavyje susijusio tinklo, kuriuo palaikomos Įstaigos operacijos, dalis;

4.6. **IRT turtas** – programinė arba techninė įranga, naudojama Įstaigos veikloje;

4.7. **operacinis arba saugumo incidentas** – pavienis įvykis arba tarpusavyje susijusių įvykių, kurių Įstaiga neplanavo ir kurie turi arba, tikėtina, turės neigiamą poveikį paslaugų vientisumui, prieinamumui, konfidencialumui ir (arba) autentiškumui, grupė;

4.8. **priimtina rizika** – bendrasis rizikos, kurią siekdamos savo strateginių tikslų Įstaigos nori prisiimti, lygis ir rūšys, atsižvelgiant į jų pajėgumą prisiimti riziką ir verslo modelį;

4.9. **trečioji šalis** – subjektas, su kuriuo Įstaiga užmezgusi verslo santykius ar sudariusi sutartis dėl produkto ar paslaugos teikimo, įskaitant rangovus ir tieikėjus;

4.10. **Įstaigos organas** – Įstaigos stebėtojų taryba, valdyba arba vienasmenis valdymo organas, kurie pagal teisės aktų reikalavimus ir Įstaigos vidaus dokumentus, yra atsakingi už Apraše nustatytų reikalavimų įgyvendinimą.

5. Įstaiga Apraše nustatytus reikalavimus taiko proporcingai, atsižvelgdama į savo dydį, organizacinę struktūrą ir veiklos (t. y. į Įstaigos teikiamų ar planuojamų teikti paslaugų) pobūdį, mastą, sudėtingumą ir rizikingumą.

II SKYRIUS
IRT IR SAUGUMO RIZIKOS VALDYMAS IR STRATEGIJA

PIRMASIS SKIRSNIS
VALDYMAS

6. Įstaiga turi užtikrinti, kad IRT ir saugumo rizikai valdyti Įstaiga turėtų tinkamą vidaus valdymo sistemą, o IRT ir saugumo rizikos nustatymas ir valdymas būtų įtrauktas į Įstaigos vidaus kontrolės sistemą.

7. Įstaiga vidaus dokumentuose turi nustatyti aiškias su IRT užduotimis, informacijos saugumo rizikos valdymu ir veiklos tęstinumu susijusias funkcijas ir pareigas, įskaitant Įstaigos organo ir, jei taikoma, Įstaigoje įsteigtų komitetų funkcijas ir pareigas.

8. Įstaiga turi užtikrinti, kad jos darbuotojų skaičius ir įgūdžiai nuolat atitiktų IRT operacinius poreikius bei IRT ir saugumo rizikos valdymo procesus ir būtų pakankami, kad būtų užtikrintas IRT strategijos įgyvendinimas, ir turėti pakankamą biudžetą šiems tikslams įgyvendinti. Įstaiga turi užtikrinti, kad visi darbuotojai būtų kasmet arba prireikus dažniau tinkamai mokomi, kad turėtų IRT ir saugumo rizikos srities, įskaitant informacijos saugumo sritį, žinių.

ANTRASIS SKIRSNIS
STRATEGIJA

9. Įstaiga turi parengti, patvirtinti Įstaigos IRT strategiją ir ją suderinti su bendra Įstaigos veiklos strategija.

10. IRT strategijoje, be kita ko, turi būti numatyta:

10.1. kaip turi būti plėtojamos Įstaigos IRT, siekiant įgyvendinti Įstaigos veiklos strategiją, įskaitant organizacinės struktūros, IRT sistemos pokyčius ir ryšius su trečiosiomis šalimis;

10.2. planuojama IRT architektūros strategija ir raida, įskaitant priklausomybės nuo trečiųjų šalių ryšius;

10.3. aiškūs informacijos saugumo tikslai, sutelkiant dėmesį į IRT sistemas ir IRT paslaugas, darbuotojus ir procesus.

11. Įstaiga turi parengti veiksmų planą su numatytomis priemonėmis, skirtomis IRT strategijos tikslams įgyvendinti, ir su juo supažindinti visus susijusius darbuotojus, įskaitant, jei taikoma, trečiąsias šalis. Veiksmų planas turi būti reguliariai persvarstomas, siekiant užtikrinti jo aktualumą ir tinkamumą.

12. Įstaiga turi įdiegti IRT strategijos veiksmingumo ir įgyvendinimo stebėsenos ir vertinimo procesus.

TREČIASIS SKIRSNIS
TREČIŲJŲ ŠALIŲ TEIKĖJŲ PASITELKIMAS

13. Įstaiga turi užtikrinti IRT ir saugumo rizikos mažinimo priemonių veiksmingumą, kaip numatyta jų rizikos valdymo sistemoje, įskaitant Apraše nustatytas priemones, kai operacinės mokėjimo paslaugų ir (arba) IRT paslaugų ir bet kurios veiklos rūšies IRT sistemų funkcijos užsakomos, be kita ko, iš Įstaigos grupei priklausančių subjektų arba kai pasitelkiamos trečiosios šalys.

14. Siekdama užtikrinti IRT paslaugų ir IRT sistemų tęstinumą, Įstaiga turi užtikrinti, kad su trečiosiomis šalimis arba Įstaigos grupės subjektais sudarytose sutartyse ir susitarimuose dėl paslaugų lygio (ir įprastomis aplinkybėmis, ir sutrikus paslaugų teikimui), be kita ko, būtų numatyta:

14.1. tinkami ir proporcingi su informacijos saugumu susiję tikslai ir priemonės, įskaitant tokius reikalavimus kaip minimalieji kibernetinio saugumo reikalavimai, specifikacijos dėl Įstaigos duomenų saugojimo terminų, duomenų šifravimo, tinklo saugumo ir saugumo stebėsenos procesų, duomenų centrų buvimo vietos reikalavimai;

14.2. operacinių ir saugumo incidentų valdymo procedūros, įskaitant problemų sprendimo ir suinteresuotų šalių informavimo procedūras.

15. Įstaiga turi vykdyti nuolatinę trečiųjų šalių stebėseną, kad įsitikintų, jog taikomos Įstaigos nustatytos priemonės, siekiama saugumo ir veikos tikslų.

III SKYRIUS
IRT IR SAUGUMO RIZIKOS VALDYMO SISTEMA

PIRMASIS SKIRSNIS
VALDYMO ORGANIZAVIMAS

16. Įstaiga IRT ir saugumo rizikai valdyti turi taikyti trijų veiksmingų gynybos linijų (vidaus valdymo ir kontrolės, rizikos valdymo ir vidaus audito) modelį.

17. Įstaiga turi nustatyti ir valdyti savo IRT ir saugumo riziką. IRT funkcija (-os), kuriai priskirta atsakomybė už IRT sistemas, procesus ir saugumo operacijas, turi numatyti 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 Įstaigos priimtinos rizikos ribų, kad rengiami projektai ir sistemos, vykdoma veikla atitiktų teisės aktų ir Įstaigos vidaus dokumentų reikalavimus.

18. Įstaiga turi užtikrinti, kad atsakomybė už IRT ir saugumo rizikos valdymą ir priežiūrą būtų priskirta kontrolės funkcijai. Tokia kontrolės funkcija turi būti nepriklausoma ir objektyvi, atskirta nuo IRT vykdomų operacijų procesų. Už šią kontrolės funkciją turi būti tiesiogiai atsiskaitoma Įstaigos organui. Ši kontrolės funkcija turi apimti atsakomybę už IRT ir saugumo rizikos valdymo sistemos stebėseną ir kontrolę. Ji turi užtikrinti, kad IRT ir saugumo rizika nustatoma, matuojama, vertinama, valdoma ir stebima ir kad apie ją pranešama. Įstaiga, jei taikoma, turi užtikrinti, kad tokia kontrolės funkcija atskirta nuo vidaus audito funkcijos.

19. Taikydamas rizika pagrįstą metodą, vidaus auditą atliekantis asmuo turi gebėti nepriklausomai peržiūrėti ir objektyviai įvertinti visos su IRT ir saugumu susijusios veiklos, įskaitant Įstaigos padalinių veiklą, atitiktį Įstaigos politikų, procedūrų ir teisės aktų reikalavimams.

20. Siekdama užtikrinti, kad IRT ir saugumo rizikos valdymo sistema būtų veiksminga, Įstaiga turi apibrėžti ir priskirti pagrindines funkcijas ir pareigas bei nustatyti atitinkamas atskaitomybės linijas. Tokia sistema turi būti visiškai integruota į bendrus Įstaigos rizikos valdymo procesus ir su jais suderinta.

21. IRT ir saugumo rizikos valdymo sistemoje turi būti įdiegti procesai, kad būtų galima:

21.1. nustatyti priimtiną IRT ir saugumo rizikos lygį, atsižvelgiant į Įstaigai priimtiną riziką;

21.2. nustatyti ir įvertinti Įstaigai kylančią IRT ir saugumo riziką;

21.3. nustatyti IRT ir saugumo rizikos mažinimo ir kontrolės priemones;

21.4. stebėti įdiegtų priemonių veiksmingumą ir incidentų, apie kuriuos pranešama, skaičių, įskaitant incidentus, kurie daro poveikį su IRT susijusiai veiklai, ir prireikus imtis veiksmų, siekiant pakoreguoti priemones;

21.5. informuoti Įstaigos organą apie IRT ir saugumo riziką ir kontrolės priemones;

21.6. nustatyti ir įvertinti, ar dėl svarbių IRT sistemos arba IRT paslaugų, procesų ar procedūrų pakeitimų ir (arba) po svarbaus operacinio ar saugumo incidento kyla IRT ir saugumo rizika.

22. Įstaiga turi dokumentuoti IRT ir saugumo rizikos valdymo sistemą ir nuolat ją atnaujinti vadovaudamasi patirtimi, įgyta ją įgyvendinant ir vykdant jos stebėseną. Įstaigos IRT ir saugumo rizikos valdymo sistema turi būti ne rečiau kaip kartą per metus peržiūrima ir patvirtinama Įstaigos organo.

ANTRASIS SKIRSNIS
FUNKCIJŲ, PROCESŲ IR IŠTEKLIŲ NUSTATYMAS

23. Siekdama nustatyti kiekvieno su IRT ir saugumo rizika susijusio tarpusavio priklausomybės ryšio svarbą, Įstaiga turi parengti ir nuolat atnaujinti savo veiklos funkcijų, atsakingų vykdytojų ir pagalbinių procesų žemėlapį.

24. Siekdama valdyti bent kritinių veiklos funkcijų ir procesų informacinius išteklius, Įstaiga turi parengti ir nuolat atnaujinti informacinių išteklių, kuriais grindžiamos jos veiklos funkcijos ir pagalbiniai procesai (IRT sistemos, darbuotojai, rangovai, trečiosios šalys ir priklausomybė nuo kitų vidaus ir išorės sistemų ir procesų), registrą. Informacinių išteklių registre turi būti aiškiai priskirta Įstaigos darbuotojų atskaitomybė ir atsakomybė už kiekvieną informacinį išteklių (inventorizavimas, klasifikavimas, apsauga, prieigų valdymas, tinkamas tvarkymas, kai išteklius pašalinamas ar sunaikinamas, ir pan.).

TREČIASIS SKIRSNIS
KLASIFIKAVIMAS IR RIZIKOS VERTINIMAS

25. Įstaiga turi klasifikuoti veiklos funkcijas, pagalbinius procesus ir informacinius išteklius pagal jų svarbą, atsižvelgdama į konfidencialumo, vientisumo ir prieinamumo reikalavimus.

26. Įstaiga turi įvertinti IRT ir saugumo riziką, darančią poveikį nustatytoms ir pagal svarbą klasifikuotoms veiklos funkcijoms, pagalbiniams procesams ir informaciniams ištekliams. Toks rizikos vertinimas turi būti atliekamas ir dokumentuojamas ne rečiau kaip kartą per metus. Rizikos vertinimas taip pat turi būti atliekamas iš esmės pasikeitus infrastruktūrai, procesams ar procedūroms, darančioms poveikį veiklos funkcijoms, pagalbiniams procesams arba informaciniams ištekliams, ir tada atitinkamai atnaujinamas galiojantis Įstaigos rizikos vertinimas.

27. Atlikdama rizikos vertinimą, Įstaiga turi persvarstyti, ar informaciniai ištekliai klasifikuojami tinkamai, ir peržiūrėti su tuo susijusius dokumentus.

28. Įstaiga turi užtikrinti, kad būtų nuolat vykdoma grėsmių ir pažeidžiamumo stebėsena, susijusi su jos veiklos procesais, pagalbinėmis funkcijomis ir informaciniais ištekliais, ir reguliariai persvarstyti poveikį jai darančius rizikos scenarijus.

KETVIRTASIS SKIRSNIS
RIZIKOS MAŽINIMAS

29. Vadovaudamasi rizikos vertinimu, Įstaiga turi nustatyti, kokių priemonių reikia imtis siekiant sumažinti nustatytą IRT ir saugumo riziką iki priimtino lygio ir ar būtina keisti esamus veiklos procesus, kontrolės priemones, IRT sistemas ir IRT paslaugas. Įstaiga turi įvertinti, 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 Įstaigai priimtinos IRT ir saugumo rizikos.

30. Įstaiga turi apibrėžti ir įgyvendinti nustatytas IRT ir saugumo rizikos mažinimo ir informacinių išteklių apsaugos priemones, atsižvelgdama į jų svarbą, nustatytą klasifikavimo metu.

PENKTASIS SKIRSNIS
INFORMAVIMAS

31. Įstaigos organui rizikos vertinimo rezultatai turi būti pateikiami vidaus dokumentuose nustatytu periodiškumu.

32. MPT, atlikęs Aprašo 26 punkte nurodytą rizikos vertinimą, ne vėliau kaip per 14 dienų Lietuvos bankui elektroninėmis priemonėmis turi pateikti atnaujintą ir pagal Aprašo priedą parengtą Operacinės ir saugumo rizikos vertinimo ataskaitą.

ŠEŠTASIS SKIRSNIS
AUDITAS

33. Įstaigos valdymą, sistemas ir procesus, susijusius su jos IRT ir saugumo rizika, turi reguliariai tikrinti nepriklausomi ir pakankamai žinių, įgūdžių ir patirties IRT ir saugumo rizikos ir mokėjimų srityje turintys vidaus ar išorės auditoriai ir Įstaigos organui pateikti nepriklausomą išvadą dėl jų veiksmingumo. Tokių auditų dažnio ir srities parinkimas turi būti proporcingas IRT ir saugumo rizikai.

34. Įstaiga į Įstaigos organo tvirtinamą audito planą turi įtraukti visus numatomus IRT auditus ir svarbius jo pakeitimus. Audito planas ir jo įgyvendinimas, įskaitant audito dažnį, turi atspindėti Įstaigai būdingą IRT ir saugumo riziką ir būti jai proporcingas bei reguliariai atnaujinamas.

35. Įstaiga turi įgyvendinti audito ataskaitoje nustatytų trūkumų pašalinimo pažangos stebėjimo procesą, apimantį kritinių IRT audito pastabų patikrinimą ir ištaisymą laiku.

IV SKYRIUS
INFORMACIJOS SAUGUMAS

PIRMASIS SKIRSNIS
INFORMACIJOS SAUGUMO POLITIKA

36. Įstaiga turi patvirtinti informacijos saugumo politiką (toliau – Politika), kurioje nustatyti principai ir taisyklės, skirtos apsaugoti Įstaigos ir jos klientų duomenų ir informacijos konfidencialumą, vientisumą ir prieinamumą. Politika turi atitikti Įstaigos informacijos saugumo tikslus ir būti grindžiama atitinkamais rizikos vertinimo rezultatais, su Politika turi būti supažindinti visi Įstaigos darbuotojai ir trečiosios šalys.

37. Politikoje, be kita ko, turi būti:

37.1. pagrindinių informacijos saugumo valdymo srities funkcijų ir pareigų aprašymas;

37.2. reikalavimai darbuotojams ir trečiosioms šalims;

37.3. su informacijos saugumu susijusių procesų ir technologų reikalavimai, darant prielaidą, kad už Įstaigos informacijos saugumą atsako visų lygmenų darbuotojai ir trečiosios šalys;

37.4. reikalavimai, padėsiantys užtikrinti Įstaigos kritiniais pripažintų loginių ir fizinių turto objektų, išteklių ir saugomų, perduodamų ar naudojamų neskelbtinų duomenų konfidencialumą, vientisumą ir prieinamumą.

38. Vadovaudamasi Politika, Įstaiga turi sukurti ir įgyvendinti saugumo priemones, kuriomis būtų mažinama jai kylanti IRT ir saugumo rizika. Šios priemonės turėtų apimti:

38.1. IRT ir saugumo rizikos valdymą;

38.2. loginį saugumą;
38.3. fizinį saugumą;
38.4. IRT operacijų saugumą;
38.5. saugumo stebėseną;
38.6. informacijos saugumo peržiūras, vertinimą ir testavimus;
38.7. informacijos saugumo mokymus ir informuotumo didinimą.

ANTRASIS SKIRSNIS
LOGINĖS PRIEIGOS APSAUGA

39. Įstaiga turi apibrėžti, dokumentuoti ir įgyvendinti loginės prieigos kontrolės (tapatybės ir prieigos valdymo) procedūras. Šios procedūros turi būti įgyvendinamos, kontroliuojamos, stebimos ir reguliariai persvarstomos bei apimti anomalijų stebėsenos kontrolės priemones. Tokiose procedūrose turi būti bent jau šie elementai:

39.1. būtinybė žinoti, mažiausios privilegijos ir pareigų atskyrimas – Įstaiga turi valdyti prieigos prie informacinių išteklių ir juos palaikančių sistemų teises, įskaitant nuotolinę prieigą, remdamasi principu „būtina žinoti“;

39.2. IRT sistemų vartotojams turi būti suteikiamos minimalios prieigos teisės, reikalingos jų būtinoms pareigoms vykdyti („mažiausios privilegijos“ principas), t. y. siekiant užkirsti kelią nepagrįstai prieigai prie didelio duomenų kiekio arba prieigos teisių derinių paskirstymui, nes tuo gali būti naudojamasi siekiant išvengti kontrolės priemonių („pareigų atskyrimo“ principas);

39.3. IRT sistemų vartotojų atskaitomybė – Įstaiga turi kuo labiau riboti bendrų ir pasidalijamų vartotojų paskyrų naudojimą ir užtikrinti, kad IRT sistemose atliekant veiksmus būtų galima nustatyti vartotojų tapatybę;

39.4. privilegijuotos prieigos teisės – Įstaiga turi įgyvendinti griežtas privilegijuotos prieigos prie sistemos kontrolės priemones, griežtai ribodama ir įdėmiai stebėdama padidintas prieigos prie sistemos teises turinčias paskyras (pvz., administratorių paskyras). Siekiant užtikrinti saugų ryšį ir sumažinti riziką, nuotolinė administracinė prieiga prie kritinių IRT sistemų turi būti suteikta tik pagal principą „būtina žinoti“ ir naudojant patikimus autentiškumo patvirtinimo sprendimus;

39.5. IRT sistemų vartotojų veiksmų įrašymas į žurnalą (angl. *log*) – į žurnalą turi būti įrašomi ir stebimi visi IRT sistemų privilegijuotų vartotojų veiksmai. Siekiant užkirsti kelią nesankcionuotam duomenų pakeitimui arba ištrynimui, prieigos registracijos žurnalus reikia saugoti tiek, kiek proporcinga atsižvelgiant į nustatytą veiklos funkcijų, pagalbinių procesų ir informacinių išteklių svarbą, nepažeidžiant teisės aktuose nustatytų informacijos saugojimo reikalavimų. Įstaiga turi naudoti šią informaciją siekdama palengvinti anomalios veiklos, pastebėtos teikiant paslaugas, nustatymą ir tyrimą;

39.6. prieigos valdymas – prieigos teises reikia suteikti, atšaukti arba keisti laiku, vadovaujantis iš anksto nustatytu patvirtinimo procesu, kuriame dalyvauja informacijos, prie kurios prieinama, veiklos savininkas (informacijos savininkas). Nutraukus darbo santykius ar verslo santykius, prieigos teisės turi būti nedelsiant panaikinamos;

39.7. periodinės prieigų peržiūros – prieigos teises reikia reguliariai peržiūrėti siekiant užtikrinti, kad IRT sistemų vartotojai neturėtų pernelyg didelių privilegijų ir kad prieigos teisės būtų panaikinamos nedelsiant, kai jų nebereikia;

39.8. autentiškumo patvirtinimo būdai – Įstaiga turi naudoti autentiškumo patvirtinimo būdus, kurie yra pakankamai patikimi, kad būtų galima tinkamai ir veiksmingai užtikrinti prieigų kontrolės politikos ir procedūrų laikymąsi. Autentiškumo patvirtinimo būdai turi atitikti IRT sistemų, informacijos ar proceso, prie kurio prieinama, svarbą. Atsižvelgiant į atitinkamą riziką, turi būti naudojami sudėtingi slaptažodžiai arba patikimesni autentiškumo patvirtinimo būdai (pvz., dviejų faktorių autentiškumo patvirtinimas).

40. Elektroninė taikomųjų programų prieiga prie duomenų ir IRT sistemų turi būti kuo labiau ribojama ir suteikiama tik tada, kai tai yra būtina tam tikrai paslaugai teikti.

TREČIASIS SKIRSNIS
FIZINIS SAUGUMAS

41. Siekiant apsaugoti Įstaigos patalpas, duomenų centrus ir kitas saugumo zonas, t. y. vietas, kuriose laikoma įslaptinta ar ypač svarbi informacija arba informacijos apdorojimo priemonės, nuo nesankcionuotos prieigos ir aplinkos pavojų, turi būti įgyvendintos Įstaigos vidaus dokumentuose apibrėžtos fizinio saugumo priemonės.

42. Fizinė prieiga prie IRT sistemų turi būti leidžiama tik įgaliotiems asmenims. Įgaliojimai turi būti suteikiami atsižvelgiant į asmeniui priskirtas užduotis ir atsakomybės sritis ir tik asmenims, kurie yra tinkamai išmokyti ir prižiūrimi. Siekiant užtikrinti, kad nereikalingos prieigos teisės būtų greitai panaikinamos, fizinė prieiga turi būti reguliariai peržiūrima.

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

KETVIRTASIS SKIRSNIS
IRT OPERACIJŲ SAUGUMAS

44. Siekdama užkirsti kelią saugumo problemoms, Įstaiga turi sukurti ir įgyvendinti procedūras, mažinančias IRT sistemų ir IRT paslaugų saugumo įvykių poveikį IRT. Šios procedūros turi apimti:

44.1. galimų pažeidžiamumų, kuriuos reikia įvertinti ir ištaisyti, nustatymą, užtikrinant programinės ir programinės aparatinės įrangos, įskaitant programinę įrangą, kurią Įstaiga tiekia savo darbuotojams ir išorės IRT sistemų vartotojams, diegiant kritinius saugumo atnaujinimus arba kompensuojamąsias kontrolės priemones, atnaujinimą laiku;

44.2. saugios visų tinklo komponentų bazinės konfigūracijos įgyvendinimą;

44.3. tinklo suskirstymą į segmentus, duomenų praradimo prevencijos sistemas ir tinklo srauto šifravimą, atsižvelgiant į duomenų klasifikaciją;

44.4. galutinių įrenginių, įskaitant serverius, kompiuterizuotas darbo vietas ir mobiliuosius prietaisus, apsaugos įgyvendinimą. Prieš suteikdama galutiniams įrenginiams prieigą prie tinklo, Įstaiga turi įvertinti, ar jie atitinka nustatytus saugumo standartus;

44.5. programinės įrangos, programinės aparatinės įrangos ir duomenų vientisumo patikrinimo mechanizmų įdiegimą;

44.6. saugomų ir perduodamų duomenų šifravimą, atsižvelgiant į duomenų klasifikaciją.

45. Įstaiga turi nuolat vertinti, ar veiklos aplinkos pokyčiai turi įtakos įgyvendinamoms saugumo priemonėms arba ar reikia taikyti papildomas priemones, siekiant tinkamai mažinti susijusią riziką. Šie pakeitimai turi būti įtraukti į Įstaigos pokyčių valdymo procesą, jie turi būti tinkamai planuojami, testuojami, registruojami dokumentuose, tvirtinami ir taikomi.

PENKTASIS SKIRSNIS
SAUGUMO STEBĖSENA

46. Įstaiga turi turėti procedūras, skirtas neįprastiems veiksmams, kurie gali daryti poveikį Įstaigos informacijos saugumui, nustatyti ir tinkamai reaguoti į tokius įvykius. Vykdydama nuolatinę stebėseną, Įstaiga turi įdiegti 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, be kita ko, turi apimti:

46.1. svarbius vidaus ir išorės veiksnius, įskaitant veiklos ir IRT administracines funkcijas;

46.2. operacijas, skirtas netinkamos trečiųjų šalių arba kitų subjektų prieigos ir netinkamos vidaus prieigos atvejams nustatyti;

46.3. galimas vidaus ir išorės grėsmes.

47. Įstaiga turi sukurti ir įgyvendinti procesus ir turėti organizacinę struktūrą saugumo grėsmėms, galinčioms daryti reikšmingą poveikį jos gebėjimams teikti paslaugas, nustatyti ir nuolatinei jų stebėsenai. Įstaiga turi nuolat stebėti technologijų vystymąsi, rinkti informaciją apie saugumo riziką, taip pat įgyvendinti saugumo grėsmių aptikimo priemones, siekiant aptikti galimą informacijos nutekėjimą, kenkėjišką kodą ir kitas saugumo grėsmes, taip pat viešai žinomus programinės ir techninės įrangos pažeidžiamumus, ir tikrinti, ar yra įdiegti atitinkami nauji saugumo atnaujinimai.

48. Vykdydama saugumo stebėseną, Įstaiga turi išnagrinėti operacinių ar saugumo incidentų prigimtį, nustatyti šių incidentų raidos tendencijas ir atlikti incidentų priežaščių nustatymo tyrimus.

ŠEŠTASIS SKIRSNIS
INFORMACIJOS SAUGUMO PERŽIŪROS, VERTINIMAS IR TESTAVIMAI

49. Siekdama užtikrinti veiksmingą IRT sistemų ir IRT paslaugų pažeidžiamumų nustatymą, Įstaiga turi atlikti įvairias informacijos saugumo peržiūras, vertinimus ir testavimus (pvz., atlikti grėsmių analizę, vadovaudamasi informacijos saugumo standartais, atitikties peržiūromis, vidaus ir išorės informacinių sistemų auditais arba fizinio saugumo peržiūromis). Įstaiga turi nagrinėti gerosios praktikos pavyzdžius, t. y. programinio kodo peržiūras, pažeidžiamumų vertinimus, įsiskverbimų testavimus ir raudonosios komandos pratybas (angl. *red team excercise*).

50. Įstaiga turi 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.

51. Įstaiga turi užtikrinti, kad informacijos saugumo testavimai:

51.1. būtų atliekami nepriklausomų testuotojų, turinčių pakankamai žinių, įgūdžių ir patirties testuojant informacijos saugumo priemones ir nedalyvavusių jas kuriant;

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

52. Įstaiga turi atlikti einamuosius ir pakartotinius saugumo priemonių testavimus. Visų kritinių IRT sistemų atveju tokie testavimai turi būti atliekami ne rečiau kaip kartą per metus. Nekritinės sistemos turi būti testuojamos reguliariai, taikant rizika pagrįstą metodą, bet ne rečiau kaip kartą per trejus metus.

53. MPT einamieji ir pakartotiniai saugumo priemonių testavimai atliekami vykdant išsamų su teikiamomis mokėjimo paslaugomis susijusios saugumo rizikos vertinimą.

54. Įstaiga turi užtikrinti, kad saugumo priemonių testavimai būtų atliekami pasikeitus infrastruktūrai, procesams ar procedūroms ir padarius pakeitimus dėl svarbių operacinių ar saugumo incidentų arba pradėjus naudoti naujas ar iš esmės pakeistas kritines internetines taikomąsias programas.

55. Atlikdama testavimus, Įstaiga turi remtis pastebėtomis saugumo grėsmėmis, atsižvelgti į padarytus pakeitimus ir įtraukti svarbių ir žinomų potencialių atakų scenarijus.

56. Įstaiga turi stebėti ir vertinti saugumo testavimų rezultatus ir atitinkamai atnaujinti savo saugumo priemones ir, jeigu tai susiję su kritinių IRT sistemų priemonėmis, tai daryti nedelsdama.

57. MPT testavimo sistema, be kita ko, turi apimti saugumo priemones, susijusias su:

57.1. mokėjimo terminalais ir prietaisais, naudojamais mokėjimo paslaugoms teikti;

57.2. mokėjimo terminalais ir prietaisais, naudojamais mokėjimo paslaugų vartotojų autentiškumui patvirtinti;

57.3. prietaisais ir programine įranga, kurią MPT teikia mokėjimo paslaugų vartotojų autentiškumo patvirtinimo kodams generuoti (gauti).

SEPTINTASIS SKIRSNIS
MOKYMAI IR INFORMUOTUMO DIDINIMAS

58. Siekdama užtikrinti visų darbuotojų ir trečiųjų šalių pasirengimą vykdyti savo pareigas laikantis atitinkamos saugumo politikos ir procedūrų, Įstaiga turi parengti jiems skirtą mokymo programą, įskaitant periodinio informuotumo saugumo klausimais didinimo programą, kad būtų sumažinta žmonių klaidų, vagystės, sukčiavimo, piktnaudžiavimo ar nuostolių atvejų ir pašalinta su informacijos saugumu susijusi rizika. Įstaiga turi užtikrinti, kad pagal mokymo programą visi darbuotojai ir trečiosios šalys būtų mokomi ne rečiau kaip kartą per metus.

V SKYRIUS
IRT OPERACIJŲ VALDYMAS

59. Įstaiga turi valdyti savo IRT operacijas, grindžiamas dokumentuotais ir įgyvendintais procesais ir procedūromis, patvirtintomis Įstaigos organo. Dokumentuose turi būti aprašyta, kaip Įstaiga naudoja, stebi ir valdo savo IRT sistemas ir paslaugas, įskaitant kritinių IRT operacijų dokumentavimą.

60. Įstaiga turi užtikrinti, kad jos IRT operacijų vykdymas atitiktų Įstaigos verslo poreikius. Įstaiga turi palaikyti ir, jeigu reikia, didinti savo IRT operacijų veiksmingumą, įskaitant vertinimą, kaip kuo labiau sumažinti galimas klaidas, susijusias su rankiniu būdu atliekamų užduočių vykdymu.

61. Įstaiga turi įgyvendinti kritinių IRT operacijų įrašymo į žurnalą ir stebėsenos procedūras, kad būtų galima nustatyti, analizuoti ir ištaisyti klaidas.

62. Įstaiga turi nuolat atnaujinti savo IRT išteklių (įskaitant IRT sistemas, tinklo prietaisus, duomenų bazes ir kt.) sąrašą. IRT išteklių sąraše turi būti saugoma IRT išteklių konfigūracija, nuorodos ir įvairių IRT išteklių tarpusavio priklausomybės ryšiai, kad būtų galima užtikrinti sklandų konfigūravimo ir pokyčių valdymo procesą.

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

64. Įstaiga turi stebėti ir valdyti IRT išteklių gyvavimo ciklus, siekdama užtikrinti, kad jie ir toliau atitiktų verslo poreikius ir rizikos valdymo reikalavimus. Įstaiga turi stebėti, ar trečiosios šalys arba paslaugų teikėjai, kurie yra Įstaigos grupės subjektai, palaiko jų IRT išteklius ir ar remiantis dokumentuotais procesais taikomos visos reikiamos tobulinimo ir modernizavimo priemonės. Su pasenusiais ar nepalaikomais IRT ištekliais susijusi rizika turi būti vertinama ir mažinama.

65. Siekdama laiku užkirsti kelią svarbioms su IRT sistemomis ir nepakankamais IRT pajėgumais susijusių veiklos rezultatų problemoms, jas nustatyti ir į jas reaguoti, Įstaiga turi įgyvendinti veiklos rezultatų ir pajėgumų planavimo ir stebėsenos procesus.

66. Įstaiga turi sukurti ir įgyvendinti duomenų ir IRT sistemų atsarginio kopijavimo ir atkūrimo procedūras, kad prireikus jas būtų galima atkurti. Atsarginio kopijavimo mastą ir dažnį Įstaiga turi nustatyti atsižvelgdama į VIII skyriaus trečiajame skirsnyje nustatytus atkūrimo reikalavimus ir į duomenų ir IRT sistemų kritiškumą. Įstaiga turi vertinti atsarginio kopijavimo mastą ir dažnį, atlikdama savo rizikos vertinimą. Be to, Įstaiga reguliariai turi atlikti atsarginio kopijavimo ir atkūrimo procedūrų testavimus.

67. Įstaiga turi užtikrinti, kad duomenų ir IRT sistemų atsarginės kopijos būtų tinkamai saugomos ir būtų laikomos pakankamai toli nuo pagrindinės duomenų ir IRT sistemų buvimo vietos, kad joms nekiltų tokia pati rizika.

VI SKYRIUS

IRT INCIDENTŲ IR PROBLEMŲ VALDYMAS

68. Įstaiga turi sukurti ir įgyvendinti incidentų ir problemų valdymo procesą, kurį taikant būtų stebimi ir įrašomi į žurnalą (angl. *log*) IRT operaciniai ir saugumo incidentai, o Įstaiga sutrikimų atveju tęstų arba laiku vėl pradėtų vykdyti kritines veiklos funkcijas ir procesus. Įstaiga vidaus dokumentuose turi nustatyti tinkamus kriterijus ir ribines vertes, kuriomis remiantis įvykiai būtų pripažinti operaciniais arba saugumo incidentais, ir ankstyvojo perspėjimo rodiklius, kurie būtų įspėjimas dėl išankstinio tokių incidentų nustatymo.

69. Siekdama kuo labiau sumažinti nepageidaujamų įvykių poveikį ir laiku užtikrinti veiklos atkūrimą, Įstaiga turi 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, taip užkertant kelią pakartotiniams incidentams.

70. Incidentų ir problemų valdymo procesas, be kita ko, turi apimti:

70.1. incidentų nustatymo, sekimo, įrašymo į žurnalą (angl. *log*), suskirstymo į kategorijas ir klasifikavimo pagal prioritetus procedūras, atsižvelgiant į jų svarbą veiklai;

70.2. funkcijas ir pareigas pagal įvairius incidentų scenarijus (pvz., susijusius su klaidomis, trikdžiais, kibernetinėmis atakomis);

70.3. problemų valdymo procedūras, naudojamas siekiant nustatyti, analizuoti ir pašalinti pagrindinę vieno ar kelių incidentų priežastį (Įstaiga turi analizuoti operacinius ar saugumo incidentus, galinčius padaryti poveikį Įstaigai, kurie buvo nustatyti ir (arba) įvyko organizacijos viduje ir (arba) už jos ribų, ir, siekdama sumažinti būsimų incidentų tikimybę arba poveikį, turi nagrinėti tokios analizės išvadas ir atitinkamai atnaujinti saugumo priemones);

70.4. veiksmingus vidaus komunikacijos planus, įskaitant pranešimo apie incidentus ir eskalavimo procedūras, apimančius ir su saugumu susijusius klientų skundus, siekiant užtikrinti, kad apie incidentus, galinčius padaryti didelį neigiamą poveikį kritinėms IRT sistemoms ir IRT paslaugoms, būtų pranešama su incidentu susijusio padalinio vadovybei ir IRT vadovybei ir kad *ad hoc* pagrindu Įstaigos organui būtų pranešama apie didelius incidentus ar bent jau apie poveikį, reagavimą ir papildomas kontrolės priemones, kurias reikia nustatyti dėl incidentų;

70.5. reagavimo į incidentus procedūras, siekiant sumažinti su incidentais susijusį poveikį ir užtikrinti, kad paslaugos būtų vėl teikiamos laiku ir saugiai;

70.6. konkrečius išorės komunikacijos planus, susijusius su kritinėmis veiklos funkcijomis ir procesais, skirtus komunikuoti ir bendradarbiauti su suinteresuotomis šalimis, kad būtų veiksmingai reaguojama į incidentą ir atkuriama veikla, laiku pateikiama reikiama informacija išorės šalims (pvz., klientams, kitiems rinkos dalyviams, priežiūros institucijoms), laikantis teisės aktuose nustatytų reikalavimų.

VII SKYRIUS
IRT PROJEKTŲ IR POKYČIŲ VALDYMAS

PIRMASIS SKIRSNIS
IRT PROJEKTŲ VALDYMAS

71. Įstaiga turi įgyvendinti programą ir (arba) projektų valdymo procesą, kuriame būtų apibrėžtos funkcijos, pareigos ir atsakomybės sritys, siekiant užtikrinti veiksmingą IRT strategijos įgyvendinimą.

72. Įstaiga turi 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.

73. Įstaiga turi parengti ir įgyvendinti IRT projektų valdymo politiką, kurioje, be kita ko, būtų nustatyta:

73.1. projekto tikslai;

73.2. funkcijos ir pareigos;
73.3. projekto rizikos vertinimas;
73.4. projekto planas, trukmė ir numatomi atlikti veiksmai;
73.5. pagrindiniai etapai;
73.6. pokyčių valdymo reikalavimai.

74. IRT projektų valdymas turi užtikrinti, kad informacijos saugumo reikalavimus analizuotų ir tvirtintų už IRT ir saugumo rizikos valdymą ir priežiūrą atsakingas asmuo, nepriklausomas nuo kūrimo funkciją atliekančio asmens.

75. Įstaiga turi užtikrinti, kad į projekto grupę būtų įtraukti visų su IRT projektu susijusių sričių atstovai ir kad projekto grupė turėtų žinių, kurių reikia saugiam ir sėkmingam projekto įgyvendinimui užtikrinti.

76. Įstaiga IRT projektų riziką turi įtraukti į savo rizikos valdymo sistemą. Apie IRT projektų pradžią ir pažangą ir su jais susijusią riziką Įstaigos organas turi būti informuojamas pateikiant individualius arba apibendrintus duomenis, priklausomai nuo IRT projektų svarbos ir dydžio, reguliariai ir prireikus *ad hoc* pagrindu.

ANTRASIS SKIRSNIS
IRT SISTEMŲ ĮSIGIJIMAS IR KŪRIMAS

77. Įstaiga turi sukurti ir įgyvendinti IRT sistemų įsigijimo, kūrimo ir palaikymo valdymo procesą. Šis procesas turi būti paremtas rizika pagrįstu metodu.

78. Įstaiga turi užtikrinti, kad prieš įsigyjant ar sukuriant IRT sistemas, būtų aiškiai apibrėžti funkciniai ir nefunkciniai reikalavimai (įskaitant informacijos saugumo reikalavimus) ir kad šie reikalavimai būtų patvirtinti IRT sistemą užsakančio padalinio vadovo.

79. Įstaiga turi užtikrinti, kad būtų įdiegtos priemonės, kuriomis būtų mažinama nenumatyto IRT sistemų pakeitimo arba tyčinio manipuliavimo jomis rizika IRT sistemų kūrimo ir įdiegimo į gamybos aplinką metu.

80. Įstaigoje turi būti įgyvendinta IRT sistemų testavimo ir patvirtinimo, prieš pradedant jas naudoti, metodika. Metodikoje turi būti atsižvelgiama į veiklos procesų ir išteklių svarbą. Įstaiga turi užtikrinti, kad, atlikus testavimus, naujos IRT sistemos veiktų, kaip numatyta. Testavimo metu turi būti naudojama aplinka, atitinkanti gamybos aplinką.

81. Įstaiga turi atlikti IRT sistemų, IRT paslaugų ir informacijos saugumo priemonių testavimus, kad nustatytų galimus saugumo trūkumus, pažeidimus ir incidentus.

82. Įstaiga turi įdiegti atskirą IRT aplinką, kad užtikrintų tinkamą pareigų atskyrimą ir sumažintų nepatikrintų pokyčių gamybos sistemoms poveikį, t. y. Įstaiga turi užtikrinti gamybos aplinkos atskyrimą nuo kūrimo, testavimo ir kitos ne gamybos aplinkos. Įstaiga turi užtikrinti gamybos duomenų vientisumą ir konfidencialumą ne gamybos aplinkoje. Prieiga prie gamybos duomenų turi būti suteikta tik leidimus turintiems IRT sistemų vartotojams.

83. Įstaiga turi įdiegti Įstaigos viduje kuriamų IRT sistemų programinių kodų vientisumo apsaugos priemones. Siekdama sumažinti priklausomybę nuo konkrečių sričių ekspertų, Įstaiga taip pat turi išsamiai dokumentuoti IRT sistemų kūrimą, diegimą, veikimą ir (arba) konfigūravimą. IRT sistemų dokumentacija, jei taikoma, turi apimti IRT sistemų vartotojų instrukciją, techninę sistemų dokumentaciją ir eksploatacijos procedūras.

84. Įstaigoje įdiegti IRT sistemų įsigijimo ir kūrimo procesai taip pat turi būti taikomi IRT sistemoms, kurias, taikydami rizika pagrįstą metodą, kuria arba valdo IRT organizacinei struktūrai nepriklausantys vartotojai (pvz., vartotojo skaičiavimo programos). Įstaiga turi pildyti tokių taikomųjų programų, palaikančių kritines veiklos funkcijas ar procesus, registrą.

TREČIASIS SKIRSNIS
IRT POKYČIŲ VALDYMAS

85. Siekdama užtikrinti, kad visi IRT sistemų pakeitimai būtų registruojami, testuojami, vertinami, patvirtinami, įdiegiami ir patikrinami užtikrinant kontrolę, Įstaiga turi sukurti ir įgyvendinti IRT pokyčių valdymo procesą. Įstaiga turi valdyti IRT pokyčius ekstremaliųjų situacijų atveju (t. y. pokyčius, kuriuos reikia įdiegti kuo skubiau), laikydamasi procedūrų, kurios užtikrina tinkamas apsaugos priemones.

86. Įstaiga turi vertinti, ar dabartinės veiklos aplinkos pokyčiai daro įtaką turimoms saugumo priemonėms arba reikalauja papildomų susijusios rizikos mažinimo priemonių. Tokie pokyčiai turi būti vykdomi pagal vidaus dokumentuose įtvirtintą Įstaigos pokyčių valdymo procesą.

VIII SKYRIUS
VEIKLOS TĘSTINUMO VALDYMAS

87. Siekdama rimtų veiklos sutrikimų atveju užtikrinti kuo didesnį įstaigos pajėgumą nepertraukiamai vykdyti veiklą ir apriboti nuostolius, Įstaiga turi sukurti patikimą veiklos tęstinumo valdymo procesą.

88. Veiklos tęstinumo valdymo procesas apima poveikio veiklai analizę, veiklos tęstinumo planų rengimą, reagavimo ir atkūrimo planų rengimą, šių planų testavimą ir informavimo krizės atveju priemones.

PIRMASIS SKIRSNIS
POVEIKIO VEIKLAI ANALIZĖ

89. Siekdama užtikrinti patikimą veiklos tęstinumo valdymą, Įstaiga turi atlikti poveikio veiklai analizę, vertindama jai kylančią rimtų veiklos sutrikimų riziką, kiekybiškai ir kokybiškai vertindama jų galimą poveikį konfidencialumui, vientisumui ir prieinamumui, remdamasi vidaus ir (arba) išorės duomenimis (pvz., trečiųjų šalių duomenimis, kurie yra svarbūs veiklos procesui, arba viešai prieinamais duomenimis, kurie gali būti svarbūs poveikio veiklai analizei) ir scenarijų analize. Atliekant poveikio veiklai analizę taip pat turi būti atsižvelgta į nustatytų ir klasifikuotų veiklos funkcijų, pagalbinių procesų, trečiųjų šalių ir informacinių išteklių svarbą ir jų tarpusavio priklausomybės ryšius.

90. Įstaiga turi užtikrinti, kad jos IRT sistemos ir IRT paslaugos būtų sukurtos atsižvelgiant į poveikio veiklai analizę, pavyzdžiui, numatant tam tikrų kritinių komponentų dubliavimą, kad būtų užkirstas kelias sutrikimams dėl įvykių, darančių poveikį tiems komponentams.

ANTRASIS SKIRSNIS
VEIKLOS TĘSTINUMO PLANAVIMAS

91. Remdamasi atlikta poveikio veiklai analize, Įstaiga turi parengti veiklos tęstinumą užtikrinančius planus (veiklos tęstinumo planus), juos turi patvirtinti Įstaigos organas. Planuose turi būti išsamiai nagrinėjama rizika, kuri galėtų padaryti neigiamą poveikį IRT sistemoms ir IRT paslaugoms. Planai turi padėti apsaugoti ir, jei būtina, naujai apibrėžti veiklos funkcijų, pagalbinių procesų ir informacinių išteklių konfidencialumą, vientisumą ir prieinamumą. Rengdama tokius planus, Įstaiga, kai reikia, turi tai koordinuoti su atitinkamomis suinteresuotosiomis šalimis.

92. Įstaiga turi įgyvendinti veiklos tęstinumo planus, kad užtikrintų gebėjimą tinkamai reaguoti į galimų sutrikimų scenarijus ir pašalinus sutrikimus vėl pradėtų vykdyti savo kritinę veiklą, neviršydama nustatyto atkūrimo termino (t. y. ilgiausio laikotarpio, per kurį sistemą ar procesą būtina atkurti po incidento (RTO) ir nustatyto atkūrimo momento (t. y. ilgiausio laikotarpio, per kurį dėl incidento duomenų praradimas laikomas priimtinu (RPO).

93. Atsiradus reikšmingų veiklos sutrikimų, kai tenka laikytis konkrečių veiklos tęstinumo planų, remdamasi rizika pagrįstu metodu, Įstaiga turi teikti pirmenybę veiklos tęstinumo veiksmams, atsižvelgdama į atliktą rizikos vertinimą.

94. Įstaiga veiklos tęstinumo planuose turi numatyti 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, Įstaiga turi aprašyti, kaip užtikrinamas IRT sistemų ir paslaugų tęstinumas ir Įstaigos informacijos saugumas.

TREČIASIS SKIRSNIS
REAGAVIMO IR ATKŪRIMO PLANAI

95. Remdamasi poveikio veiklai analize ir įmanomais scenarijais, Įstaiga turi parengti reagavimo ir atkūrimo planus. Šiuose planuose turi būti numatyta, kokiomis sąlygomis jie gali būti taikomi ir kokių veiksmų reikia imtis siekiant užtikrinti bent kritinių Įstaigoje įdiegtų IRT sistemų ir IRT paslaugų prieinamumą, tęstinumą ir atkūrimą. Reagavimo ir atkūrimo planais turi būti siekiama įgyvendinti Įstaigos operacijų atkūrimo tikslus.

96. Reagavimo ir atkūrimo planuose turi būti numatyti trumpalaikiai ir ilgalaikiai atkūrimo scenarijai. Planai turi būti:

96.1. parengti labiausiai atsižvelgiant į kritinių veiklos funkcijų, pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių atkūrimą, siekiant išvengti neigiamo poveikio Įstaigos veiklai ir finansų sistemai, įskaitant mokėjimo sistemas ir mokėjimo paslaugų vartotojus, taip pat siekiant užtikrinti neįvykdytų mokėjimo operacijų įvykdymą;

96.2. užregistruoti dokumentuose, kuriais galėtų naudotis veiklos ir veiklą palaikantys struktūriniai padaliniai ir kurie būtų lengvai prieinami nenumatytu atveju;

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

97. Reagavimo ir atkūrimo planuose taip pat turi būti vertinamos alternatyvos, kai trumpalaikis atkūrimas gali būti neįmanomas dėl sąnaudų, rizikos, logistikos ar kitų nenumatytų aplinkybių.

98. Reagavimo ir atkūrimo planuose Įstaiga turi numatyti tęstinumo priemones, švelninančias trečiųjų šalių, kurios yra itin svarbios Įstaigos IRT paslaugų tęstinumui, veiklos sutrikimus.

KETVIRTASIS SKIRSNIS
PLANŲ TESTAVIMAI

99. Įstaiga turi reguliariai atlikti savo veiklos tęstinumo planų testavimus. Įstaiga turi užtikrinti, kad kritinių veiklos funkcijų, pagalbinių procesų, informacinių išteklių ir jų tarpusavio priklausomybės ryšių (įskaitant, jei taikytina, trečiąsias šalis) veiklos tęstinumo planai būtų testuojami ne rečiau kaip kartą per metus.

100. Veiklos tęstinumo planus Įstaiga turi atnaujinti ne rečiau kaip kartą per metus, remdamasi testavimų rezultatais, surinktais duomenimis apie grėsmes ir su ankstesniais įvykiais susijusia patirtimi, taip pat pasikeitus atkūrimo tikslams (RTO ir RPO) ir (arba) pasikeitus veiklos funkcijoms, pagalbiniams procesams ir informaciniams ištekliams.

101. Atlikdama veiklos tęstinumo planų testavimus, Įstaiga turi įsitikinti, kad geba išlaikyti savo veiklos gyvybingumą, kol bus atkurtos kritinės operacijos. Veiklos tęstinumo planai turi atitikti šiuos reikalavimus:

101.1. turi apimti testavimus pagal kraštutinius, bet įmanomus scenarijus, įskaitant tuos, kurie buvo nagrinėjami rengiant veiklos tęstinumo planus (ir, jei taikoma, atlikti trečiųjų šalių teikiamų paslaugų testavimus), kritines veiklos funkcijas, pagalbinius procesus ir informacinius išteklius, perkeliant į atkūrimo po krizės aplinką ir įsitikinant, kad joje pavyksta vykdyti veiklą. Testavimų trukmė turi būti tokia, kad būtų galima įsitikinti, kad veiklos tęstinumo planas yra veiksmingas;

101.2. turi būti parengti taip, kad būtų kvestionuojamos prielaidos, kuriomis pagrįsti veiklos tęstinumo planai, įskaitant valdymo priemones ir informavimo krizės atveju planus;

101.3. turi apimti procedūras, kuriomis patikrinamas darbuotojų ir trečiųjų šalių, IRT sistemų ir IRT paslaugų gebėjimas tinkamai reaguoti pagal Aprašo 101.1 papunktyje numatytus scenarijus.

102. Testavimų rezultatus Įstaiga turi dokumentuoti, visus per testavimus nustatytus trūkumus išnagrinėti ir pašalinti bei apie juos pranešti Įstaigos organui.

PENKTASIS SKIRSNIS
KOMUNIKAVIMAS KRIZĖS SĄLYGOMIS

103. Sutrikus veiklai arba susiklosčius nenumatytai situacijai, įgyvendindama veiklos tęstinumo planus, Įstaiga turi būti įsidiegusi veiksmingas informavimo krizės atveju priemones, kad visos suinteresotosios šalys būtų laiku ir tinkamai informuotos.

IX SKYRIUS
RYŠIŲ SU MOKĖJIMO PASLAUGŲ VARTOTOJAIS VALDYMAS

104. MPT turi sukurti ir įgyvendinti procesus, kurie didintų mokėjimo paslaugų vartotojų informuotumą apie su mokėjimo paslaugomis susijusią saugumo riziką.

105. MPT turi mokėjimo paslaugų vartotojus informuoti apie su mokėjimo paslaugomis susijusią saugumo riziką, sudaryti sąlygas mokėjimo paslaugų vartotojams lengvai prieinamu būdu susipažinti su informacija apie mokėjimo paslaugų saugumo riziką ir galimas jos pasekmes, veiksnius, galinčius sukelti šią riziką, ir priemones, kurių turi imtis mokėjimo paslaugų vartotojai, siekdami sumažinti tokią riziką ir (arba) išvengti su ja susijusių galimų neigiamų pasekmių. Mokėjimo paslaugų vartotojams skirta informacija turi būti pateikta aiškia ir mokėjimo paslaugų vartotojams lengvai suprantama kalba.

106. MPT Aprašo 105 punkte nurodytą informaciją, taip pat mokėjimo paslaugų vartotojams teikiamą pagalbą ir patarimus turi periodiškai persvarstyti ir prireikus nedelsdami atnaujinti, atsižvelgdami į naujas kibernetines grėsmes ir pažeidžiamumus, taip pat į kitus mokėjimo paslaugų ir (arba) jomis besinaudojančių mokėjimo paslaugų vartotojų saugumui įtaką turinčius veiksnius (pvz., pasikeitė aktualūs teisės aktai, padaryti mokėjimo paslaugoms teikti būtini sistemų pakeitimai, galintys turėti įtakos mokėjimo paslaugų teikimui, ir pan.).

107. MPT, jeigu tai įmanoma pagal produkto ir (arba) priemonės funkcionalumą, turi sudaryti sąlygas mokėjimo paslaugų vartotojams išjungti ir vėl įjungti mokėjimų funkcijas, susijusias su MPT mokėjimo paslaugų vartotojams teikiamomis mokėjimo paslaugomis.

108. MPT, susitarę su mokėjimo paslaugų vartotoju dėl mokėjimo operacijų, vykdomų tam tikromis mokėjimo priemonėmis, išlaidų limitų, turi pasiūlyti mokėjimo paslaugų vartotojui galimybę keisti šį limitą, neviršijant didžiausio sutarto limito.

109. MPT turi suteikti mokėjimo paslaugų vartotojams galimybę gauti pranešimus apie inicijuotus ir (arba) nepavykusius bandymus inicijuoti mokėjimo operacijas, suteikdami jiems galimybę aptikti sukčiavimo ar piktnaudžiavimo jų sąskaita atvejus.

110. MPT turi nuolat informuoti mokėjimo paslaugų vartotojus apie saugumo procedūrų atnaujinimą, darantį poveikį mokėjimo paslaugų vartotojams, teikiant mokėjimo paslaugas.

111. MPT turi operatyviai ir laiku reaguoti į mokėjimo paslaugų vartotojų ar kitų asmenų žodinius ir rašytinius pranešimus apie mokėjimo paslaugų saugumo incidentus, anomalijas ir (arba) kitas aplinkybes, dėl kurių atsiranda (gali atsirasti) grėsmė mokėjimo paslaugų ar jomis besinaudojančių mokėjimo paslaugų vartotojų saugumui, ir nedelsdami suteikti mokėjimo paslaugų vartotojams konsultacijas ir kitą pagalbą, būtiną mokėjimo paslaugų ir mokėjimo paslaugų vartotojų saugumui užtikrinti. Mokėjimo paslaugų vartotojai turi būti tinkamai informuojami apie teisę gauti tokias konsultacijas ir pagalbą. Mokėjimo paslaugų vartotojo prašymu informacija šiame punkte nurodytais klausimais per protingą terminą turi būti pateikta su MPT sutartu būdu.

_____

Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo priedas

OPERACINĖS IR SAUGUMO RIZIKOS VERTINIMO ATASKAITA[1]

Eil. Nr.	Operacinės ir saugumo rizikos grėsmė	Grėsmių tikimybė	Poveikis veiklai	Prigimtinės rizikos vertinimas	Taikomos rizikos mažinimo kontrolės priemonės	Likutinės rizikos vertinimas	Planuojami ateities veiksmai rizikai mažinti
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*

Pakeitimai:

1.
Lietuvos bankas, Nutarimas
Nr. 03-123, 2021-08-19, paskelbta TAR 2021-08-19, i. k. 2021-17747
Dėl Lietuvos banko valdybos 2020 m. lapkričio 26 d. nutarimo Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“ pakeitimo

[1] MPT Aprašo 32 punkte nurodyta informacija teikiama prisijungus prie Pranešimų teikimo modulio, kuris prieinamas per nuorodą https://epaslaugos.lb.lt/suptech