Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/1774

2024 6 25

KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2024/1774

2024 m. kovo 13 d.

kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 papildomas techniniais reguliavimo standartais, kuriais nustatomos IRT rizikos valdymo priemonės, metodai, procesai bei politika ir supaprastinta IRT rizikos valdymo sistema

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentą (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 ([1]), ypač į jo 15 straipsnio ketvirtą pastraipą ir 16 straipsnio 3 dalies ketvirtą pastraipą,

kadangi:

(1) Reglamentas (ES) 2022/2554 taikomas labai įvairiems finansų sektoriaus subjektams, kurių dydis, struktūra, organizacinė vidaus struktūra, veiklos pobūdis ir sudėtingumas yra skirtingi, todėl jų sudėtingumo ar rizikos elementai yra didesni arba mažesni. Tam, kad į tą įvairovę būtų deramai atsižvelgta, visi su IRT saugumo politika, procedūromis, protokolais ir priemonėmis ir su supaprastinta IRT rizikos valdymo sistema susiję reikalavimai turėtų būti proporcingi tų finansų sektoriaus subjektų dydžiui, struktūrai, organizacinei vidaus struktūrai, pobūdžiui bei sudėtingumui ir atitinkamai rizikai;

(2) dėl tos pačios priežasties finansų sektoriaus subjektai, patenkantys į Reglamento (ES) 2022/2554 taikymo sritį, turėtų turėti tam tikro lankstumo laikydamiesi bet kurių su IRT saugumo politika, procedūromis, protokolais ir priemonėmis ir su supaprastinta IRT rizikos valdymo sistema susijusių reikalavimų. Todėl finansų sektoriaus subjektams turėtų būti leista naudotis jau turimais dokumentais, kad jie įvykdytų visus dokumentacijos reikalavimus, kylančius dėl tų reikalavimų. Vadinasi, jie turėtų būti įpareigoti konkrečią IRT saugumo politiką parengti, dokumentuoti ir įgyvendinti tik tam tikrų esminių elementų atžvilgiu, atsižvelgdami, be kita ko, į pažangiausią sektoriaus praktiką ir standartus. Be to, siekiant atsižvelgti į specifinius techninius įgyvendinimo aspektus, kaip antai pajėgumo ir veiklos rezultatų valdymą, pažeidžiamumų ir pataisų valdymą, duomenų ir sistemų apsaugą, duomenų registravimą, būtina parengti, dokumentuoti ir įgyvendinti IRT saugumo procedūras;

(3) siekiant užtikrinti, kad šio reglamento II antraštinės dalies I skyriuje nurodyta IRT saugumo politika, procedūros, protokolai ir priemonės būtų ilgainiui įgyvendinami teisingai, svarbu, kad finansų sektoriaus subjektai teisingai paskirtų ir atnaujintų visus su IRT saugumu susijusius vaidmenis bei pareigas ir nustatytų IRT saugumo politikos ar procedūrų nesilaikymo pasekmes;

(4) kad apribotų interesų konfliktų riziką, skirdami IRT vaidmenis ir pareigas finansų sektoriaus subjektai turėtų užtikrinti pareigų atskyrimą;

(5) siekiant užtikrinti lankstumą ir supaprastinti finansų sektoriaus subjektų kontrolės sistemą, tų subjektų nereikėtų įpareigoti rengti konkrečių nuostatų dėl šio reglamento II antraštinės dalies I skyriuje nurodytos IRT saugumo politikos, procedūrų ir protokolų nesilaikymo pasekmių, jei tokios nuostatos jau yra nustatytos kita politika ar procedūra;

([1]) OL L 333, 2022 12 27, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(6) svarbu, kad dinamiškoje aplinkoje, kurioje IRT rizika nuolat kinta, finansų sektoriaus subjektai savo IRT saugumo politiką kurtų remdamiesi pažangiausia praktika ir, jei yra, standartais, apibrėžtais Europos Parlamento ir Tarybos reglamento (ES) Nr. 1025/2012 ([2]) 2 straipsnio 1 punkte. Tai turėtų padėti šio reglamento II antraštinėje dalyje nurodytiems finansų sektoriaus subjektams išlikti informuotiems ir pasirengusiems kintančiomis aplinkybėmis;

(7) kad būtų užtikrintas šio reglamento II antraštinėje dalyje nurodytų finansų sektoriaus subjektų skaitmeninės veiklos atsparumas, įgyvendindami savo IRT saugumo politiką, procedūras, protokolus ir priemones šie subjektai turėtų sukurti ir įgyvendinti IRT turto valdymo politiką, pajėgumo ir veiklos rezultatų valdymo procedūras ir IRT operacijų politiką ir procedūras. Tos politikos ir procedūrų reikia siekiant užtikrinti IRT turto būklės stebėseną visą jo gyvavimo ciklą, kad tas turtas būtų naudojamas ir prižiūrimas veiksmingai (IRT turto valdymas). Be to, ta politika ir procedūromis turėtų būti užtikrinamas IRT sistemų veikimo optimizavimas ir kad IRT sistemų bei pajėgumo veiklos rezultatai atitiktų nustatytus veiklos ir informacijos saugumo tikslus (pajėgumo ir veiklos rezultatų valdymas). Galiausiai ta politika ir procedūromis turėtų būti užtikrinamas veiksmingas ir sklandus kasdienis IRT sistemų valdymas ir veikimas (IRT operacijos), kartu sumažinant duomenų konfidencialumo, vientisumo ir prieinamumo praradimo riziką. Taigi tos politikos ir procedūrų reikia siekiant užtikrinti tinklų saugumą, numatyti tinkamas apsaugos nuo įsibrovimo ir netinkamo duomenų naudojimo priemones ir išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą;

(8) siekdami užtikrinti tinkamą senųjų IRT sistemų rizikos valdymą, finansų sektoriaus subjektai turėtų registruoti ir stebėti IRT paslaugas teikiančių trečiųjų šalių teikiamų pagalbos paslaugų pabaigos datas. Finansų sektoriaus subjektai turėtų atsižvelgti į galimą duomenų konfidencialumo, vientisumo ir prieinamumo praradimo poveikį ir, registruodami ir stebėdami tas pabaigos datas, daugiausia dėmesio skirti tam IRT turtui ar sistemoms, kurie veiklos vykdymui yra ypatingos svarbos;

(9) kriptografijos kontrolės priemonėmis galima užtikrinti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą. Todėl šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų nustatyti ir įgyvendinti tokias kontrolės priemones, laikydamiesi rizika grindžiamo požiūrio. Tuo tikslu finansų sektoriaus subjektai, remdamiesi dvilypio proceso, kurį sudaro duomenų klasifikavimas ir išsamus IRT rizikos vertinimas, rezultatais, turėtų užšifruoti saugomus, perduodamus ar prireikus naudojamus duomenis. Kadangi užšifruoti naudojamus duomenis yra sudėtinga, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų naudojamus duomenis užšifruoti tik tuo atveju, jei tai būtų tikslinga atsižvelgus į IRT rizikos vertinimo rezultatus. Tačiau tais atvejais, kai naudojamų duomenų užšifravimas yra neįmanomas arba per sudėtingas, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų galėti atitinkamų duomenų konfidencialumą, vientisumą ir prieinamumą apsaugoti kitomis IRT apsaugos priemonėmis. Atsižvelgiant į sparčią kriptografinių metodų technologinę plėtrą, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų eiti koja kojon su atitinkamais kriptoanalizės pokyčiais ir domėtis pažangiausia praktika ir standartais. Taigi siekdami vykdyti veiklą dinamiškoje kriptogrėsmių, be kita ko, susijusių su kvantinių technologijų pažanga, aplinkoje šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų laikytis lankstaus požiūrio, grindžiamo rizikos mažinimu ir stebėsena;

(10) siekiant užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą, yra būtina IRT operacijų saugumo ir veiklos politika, procedūros, protokolai ir priemonės. Vienas kertinių jų aspektų – patikimai atskirti IRT produkcinę aplinką nuo tokios aplinkos, kurioje IRT sistemos yra kuriamos ir testuojamos, ar kitos neprodukcinės aplinkos. Tas atskyrimas turėtų būti taikomas kaip svarbi IRT apsaugos priemonė, padedanti išvengti nenumatytos ir neteisėtos prieigos prie duomenų, jų pakeitimo ir ištrynimo produkcinėje aplinkoje, galinčių lemti didelius šio reglamento II antraštinėje dalyje nurodytų finansų sektoriaus subjektų veiklos operacijų sutrikimus. Tačiau, atsižvelgus į dabartinę IRT sistemų kūrimo praktiką, išskirtinėmis aplinkybėmis finansų sektoriaus subjektams turėtų būti leidžiama atlikti testus produkcinėje aplinkoje, jeigu jie tokį testavimą pagrindžia ir gauna reikalingą patvirtinimą;

([2]) 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB (OL L 316, 2012 11 14, p. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

(11) dėl sparčiai kintančio IRT aplinkos, IRT pažeidžiamumų ir kibernetinių grėsmių pobūdžio reikia iniciatyvaus ir visapusiško IRT pažeidžiamumų identifikavimo, įvertinimo ir šalinimo metodo. Neturint tokio metodo, finansų sektoriaus subjektams, jų klientams, naudotojams ar sandorių šalims galėtų kilti didelė rizika, todėl jų skaitmeninės veiklos atsparumas, jų tinklų saugumas, duomenų prieinamumas, autentiškumas, vientisumas ir konfidencialumas, kuriuos IRT saugumo politika ir procedūros turėtų apsaugoti, atsidurtų pavojuje. Todėl šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų identifikuoti ir panaikinti savo IRT aplinkos pažeidžiamumus ir tiek patys finansų sektoriaus subjektai, tiek jų IRT paslaugas teikiančios trečiosios šalys turėtų laikytis nuoseklios, skaidrios ir atsakingos pažeidžiamumų valdymo sistemos. Dėl tos pačios priežasties finansų sektoriaus subjektai turėtų stebėti IRT pažeidžiamumus, naudodamiesi patikimais šaltiniais bei automatizuotomis priemonėmis ir tikrindami, ar IRT paslaugas teikiančios trečiosios šalys užtikrina skubų reagavimą į jų teikiamų IRT paslaugų pažeidžiamumus;

(12) tos IRT saugumo politikos ir procedūrų, kuriomis testavimo ir diegimo kontroliuojamoje aplinkoje būdu siekiama panaikinti identifikuotus pažeidžiamumus ir diegiant pataisas išvengti sutrikimų, esminė dalis turėtų būti pataisų valdymas;

(13) siekiant užtikrinti savalaikį ir skaidrų informacijos apie galimas grėsmes saugumui, galinčias daryti poveikį finansų sektoriaus subjektui ir jo suinteresuotiesiems subjektams, perdavimą, finansų sektoriaus subjektai turėtų nustatyti atsakingo informacijos apie IRT pažeidžiamumus atskleidimo klientams, sandorių šalims ir visuomenei procedūras. Rengdami tas procedūras, finansų sektoriaus subjektai turėtų atsižvelgti į veiksnius, be kita ko, pažeidžiamumo kritiškumą, galimą tokio pažeidžiamumo poveikį suinteresuotiesiems subjektams ir ištaisymo ar poveikio mažinimo priemonių parengtį;

(14) kad sudarytų sąlygas priskirti naudotojams prieigos teises, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų nustatyti saugesnes priemones, kuriomis pagal unikalius identifikatorius būtų tikrinama asmenų ir sistemų, turėsiančių prieigą prie finansų sektoriaus subjekto informacijos, tapatybė. To nepadariusiems finansų sektoriaus subjektams kiltų galimos neteisėtos prieigos, duomenų apsaugos pažeidimų ir nesąžiningos veiklos rizika, kelianti grėsmę neskelbtinų finansinių duomenų konfidencialumui, vientisumui ir prieinamumui. Nors išskirtinėmis finansų sektoriaus subjektų nustatytomis aplinkybėmis reikėtų leisti naudotis beasmenėmis ar bendrosiomis paskyromis, finansų sektoriaus subjektai turėtų užtikrinti, kad būtų išlaikyta atskaitomybė už veiksmus, atliktus naudojantis tomis paskyromis. Be tos apsaugos priemonės, potencialūs piktavaliai naudotojai galėtų trukdyti taikyti tyrimo ir taisomąsias priemones, todėl finansų sektoriaus subjektai būtų neapsaugoti nuo neaptiktos kenkėjiškos veiklos ar baudų už reikalavimų nesilaikymą;

(15) siekdami žengti koja kojon su sparčia IRT aplinkos pažanga, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų įgyvendinti patikimą IRT projektų valdymo politiką ir procedūras, kad išsaugotų duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą. Pagal tą IRT projektų valdymo politiką ir procedūras turėtų būti galima identifikuoti elementus, būtinus sėkmingam IRT projektų valdymui, įskaitant finansų sektoriaus subjekto IRT sistemų pakeitimus, įsigijimą, priežiūrą ir plėtojimą, nepriklausomai nuo finansų sektoriaus subjekto pasirinktos IRT projektų valdymo metodikos. Atsižvelgdami į tą politiką ir procedūras, finansų sektoriaus subjektai turėtų patvirtinti jų poreikius atitinkančią testavimo praktiką ir metodus, laikydamiesi rizika grindžiamo metodo ir užtikrindami, kad būtų išsaugota saugi, patikima ir atspari IRT aplinka. Siekdami garantuoti saugų IRT projekto įgyvendinimą, finansų sektoriaus subjektai turėtų užtikrinti, kad konkrečių veiklos sektorių ar vaidmenų, kuriems tas IRT projektas daro įtaką ar poveikį, darbuotojai galėtų suteikti būtinos informacijos ir ekspertinių žinių. Tam, kad būtų užtikrinta veiksminga priežiūra, IRT projektų ataskaitos, ypač susijusios su projektais, darančiais poveikį ypatingos svarbos arba svarbioms funkcijoms, ir su jiems būdinga rizika, turėtų būti teikiamos valdymo organui. Finansų sektoriaus subjektai turėtų nustatyti sistemingos ir nuolatinės peržiūros bei ataskaitų teikimo periodiškumą ir duomenis pagal atitinkamų IRT projektų svarbą ir dydį;

(16) būtina užtikrinti, kad šio reglamento II antraštinėje dalyje nurodytų finansų sektoriaus subjektų įsigyjami ir kuriami programinės įrangos paketai būtų veiksmingai ir saugiai integruojami į esamą IRT aplinką, laikantis nustatytų verslo ir informacijos saugumo tikslų. Todėl finansų sektoriaus subjektai turėtų tokius programinės įrangos paketus visapusiškai įvertinti. Tuo tikslu ir siekdami identifikuoti tiek programinės įrangos paketų, tiek platesnių IRT sistemų pažeidžiamumus ir galimas saugumo spragas, finansų sektoriaus subjektai turėtų IRT saugumą testuoti. Siekdami įvertinti programinės įrangos vientisumą ir užtikrinti, kad tos programinės įrangos naudojimas nekeltų IRT saugumo rizikos, finansų sektoriaus subjektai taip pat turėtų patikrinti įsigytos programinės įrangos ir, be kita ko, jei įmanoma, IRT paslaugas teikiančių trečiųjų šalių nuosavybinės programinės įrangos pirminius kodus tiek pagal statinio, tiek pagal dinaminio testavimo metodus;

(17) bet kokio masto pakeitimams yra būdinga rizika, jie gali kelti reikšmingą duomenų konfidencialumo, vientisumo ir prieinamumo praradimo riziką, todėl gali lemti didelius verslo sutrikimus. Kad finansų sektoriaus subjektai apsisaugotų nuo galimų IRT pažeidžiamumų ir trūkumų, galinčių jiems sukelti reikšmingą riziką, taikant griežtą patikrinimo procesą būtina įsitikinti, kad visi pakeitimai atitiktų privalomus IRT saugumo reikalavimus. Todėl šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų įgyvendinti patikimą IRT pakeitimų valdymo politiką ir procedūras kaip esminę savo IRT saugumo politikos ir procedūrų elementą. Kad būtų išlaikytas IRT pakeitimų valdymo objektyvumas ir veiksmingumas, užkirstas kelias interesų konfliktams ir užtikrintas objektyvus IRT pakeitimų vertinimas, būtina atskirti už tų pakeitimų tvirtinimą atsakingas funkcijas nuo tų pakeitimų prašančių ir juos įgyvendinančių funkcijų. Siekdami veiksmingo pakeitimo proceso, kontroliuojamo IRT pakeitimo įgyvendinimo ir minimalių IRT sistemų veikimo sutrikimų, finansų sektoriaus subjektai turėtų paskirti aiškius vaidmenis ir pareigas, kuriais būtų užtikrintas IRT pakeitimų planavimas, tinkamas testavimas ir kokybė. Tam, kad IRT sistemos toliau veiktų veiksmingai, o finansų sektoriaus subjektai turėtų apsaugos priemonių, finansų sektoriaus subjektai taip pat turėtų parengti ir įgyvendinti atsargines procedūras. Jie turėtų tas atsargines procedūras aiškiai identifikuoti ir priskirti pareigas, užtikrinsiančias greitą ir veiksmingą reagavimą nesėkmingų IRT pakeitimų atveju;

(18) siekdami aptikti, valdyti su IRT susijusius incidentus ir apie juos pranešti, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų nustatyti su IRT susijusių incidentų politiką, apimančią su IRT susijusių incidentų valdymo proceso komponentus. Tuo tikslu finansų sektoriaus subjektai turėtų identifikuoti visus atitinkamus kontaktinius asmenis organizacijos viduje ir išorėje, galinčius padėti tinkamai koordinuoti ir įgyvendinti įvairius to proceso etapus. Kad optimizuotų su IRT susijusių incidentų aptikimą bei reagavimą į juos ir identifikuotų tiems incidentams būdingas tendencijas, kurios yra vertingas informacijos šaltinis, padedantis finansų sektoriaus subjektams veiksmingai identifikuoti ir šalinti pagrindines priežastis ir problemas, finansų sektoriaus subjektai visų pirma turėtų detaliai išanalizuoti, jų vertinimu, pačius reikšmingiausius, be kita ko, dėl jų periodiško pasikartojimo, su IRT susijusius incidentus;

(19) siekdami užtikrinti ankstyvą ir veiksmingą neįprastos veiklos aptikimą, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų rinkti, stebėti ir analizuoti įvairių šaltinių informaciją ir priskirti susijusius vaidmenis ir pareigas. Kalbant apie vidaus informacijos šaltinius, ypač aktualus šaltinis yra registracijos įrašai, tačiau finansų sektoriaus subjektai neturėtų kliautis vien tik jais. Finansų sektoriaus subjektai turėtų apsvarstyti platesnę informaciją, apimančią tai, ką pranešė kitas vidaus funkcijas vykdantys darbuotojai, nes dažnai jie yra vertingas svarbios informacijos šaltinis. Dėl tos pačios priežasties finansų sektoriaus subjektai turėtų analizuoti ir stebėti iš išorinių šaltinių surinktą informaciją, be kita ko, IRT paslaugas teikiančių trečiųjų šalių pateiktą informaciją apie incidentus, padariusius poveikį jų sistemoms ir tinklams, ir kitų šaltinių informaciją, kurią finansų sektoriaus subjektai laiko svarbia. Kai tokia informacija apima asmens duomenis, taikoma Sąjungos duomenų apsaugos teisė. Naudojami tik tie asmens duomenys, kurie būtini incidentui aptikti;

(20) kad būtų lengviau aptikti su IRT susijusius incidentus, finansų sektoriaus subjektai turėtų išsaugoti tų incidentų įrodymus. Viena vertus, kad užtikrintų, kad tokie įrodymai būtų saugomi pakankamai ilgai ir, kita vertus, kad išvengtų pernelyg didelės reguliavimo naštos, finansų sektoriaus subjektai turėtų nustatyti saugojimo laikotarpį, atsižvelgdami, be kita ko, į ypatingą duomenų svarbą ir iš Sąjungos teisės kylančius išlaikymo reikalavimus;

(21) siekdami užtikrinti su IRT susijusių incidentų aptikimą laiku, šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai neturėtų apsiriboti nustatytais kriterijais, pagal kuriuos inicijuojamas su IRT susijusių incidentų aptikimas ir reagavimas į juos. Be to, nors finansų sektoriaus subjektai turėtų atsižvelgti į kiekvieną iš šių kriterijų, siekiant inicijuoti su IRT susijusių incidentų aptikimą ir reagavimą į juos, kriterijais apibrėžtos aplinkybės nebūtinai turėtų būti susiklosčiusios vienu metu, o paveiktų IRT paslaugų svarba turėtų būti tinkamai apsvarstyta;

(22) šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai, rengdami IRT veiklos tęstinumo politiką, turėtų atsižvelgti į IRT rizikos valdymo, įskaitant su IRT susijusių incidentų valdymo ir komunikacijos strategijas, ir IRT pakeitimų valdymo proceso esminius komponentus ir į IRT paslaugas teikiančių trečiųjų šalių keliamą riziką;

(23) būtina nustatyti tam tikrus scenarijus, į kuriuos šio reglamento II antraštinėje dalyje nurodyti finansų sektoriaus subjektai turėtų atsižvelgti tiek įgyvendindami IRT reagavimo ir veiklos atkūrimo planus, tiek testuodami IRT veiklos tęstinumo planus. Tie scenarijai turėtų būti finansų sektoriaus subjektų naudojami kaip atskaitos taškas, analizuojant tiek kiekvieno scenarijaus aktualumą ir tikėtinumą, tiek poreikį rengti alternatyvius scenarijus. Finansų sektoriaus subjektai daugiausia dėmesio turėtų skirti tiems scenarijams, pagal kuriuos investicijos į atsparumo priemones galėtų būti veiksmingesnės ir produktyvesnės. Atlikdamos pirminės IRT infrastruktūros pakeitimo bet kokiais atsarginiais pajėgumais, atsarginėmis kopijomis ir atsarginiais įrenginiais testus, finansų įstaigos turėtų įvertinti, ar tie pajėgumai, atsarginės kopijos ir įrenginiai veikia veiksmingai pakankamą laiko tarpą ir užtikrina normalaus pirminės IRT infrastruktūros funkcionavimo atkūrimą pagal atkūrimo tikslus;

(24) būtina nustatyti operacinės rizikos reikalavimus ir konkrečiau reikalavimus, taikomus IRT projektų ir pakeitimų valdymui ir IRT veiklos tęstinumo valdymui ir grindžiamus tais reikalavimais, kurie jau taikomi pagrindinėms sandorio šalims, centriniams vertybinių popierių depozitoriumams ir prekybos vietoms pagal atitinkamai Europos Parlamento ir Tarybos reglamentus (ES) Nr. 648/2012 ([3]), (ES) Nr. 600/2014 ([4]) ir (ES) Nr. 909/2014 ([5]);

(25) Reglamento (ES) 2022/2554 6 straipsnio 5 dalimi finansų sektoriaus subjektai įpareigojami peržiūrėti savo IRT rizikos valdymo sistemą ir savo kompetentingai institucijai pateikti tos peržiūros ataskaitą. Siekiant užtikrinti, kad kompetentingos institucijos galėtų lengvai tvarkyti tose ataskaitose pateiktą informaciją, ir garantuoti tinkamą tos informacijos perdavimą, finansų sektoriaus subjektai tas ataskaitas turėtų teikti elektroniniu formatu, leidžiančiu naudoti paieškos funkciją;

(26) finansų sektoriaus subjektams, kuriems taikoma supaprastinta IRT rizikos valdymo sistema, nurodyta Reglamento (ES) 2022/2554 16 straipsnyje, skirti reikalavimai turėtų būti orientuoti į svarbiausias sritis ir elementus, kurie, atsižvelgus į tų finansų sektoriaus subjektų mastą, riziką, dydį ir sudėtingumą, yra patys būtiniausi siekiant užtikrinti tų finansų sektoriaus subjektų duomenų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir autentiškumą. Tomis aplinkybėmis tie finansų sektoriaus subjektai turėtų taikyti vidaus valdymo ir kontrolės sistemą su aiškiai paskirstytomis pareigomis, kad sudarytų sąlygas turėti veiksmingą ir patikimą rizikos valdymo sistemą. Be to, kad sumažėtų administracinė ir veiklos našta, tie finansų sektoriaus subjektai turėtų parengti ir dokumentais pagrįsti tik vieną politiką, t. y. informacijos saugumo politiką, kurioje būtų nustatyti bendrieji principai ir taisyklės, būtini tų finansų sektoriaus subjektų duomenų ir paslaugų konfidencialumui, vientisumui, prieinamumui ir autentiškumui apsaugoti;

(27) šio reglamento nuostatos yra susijusios su IRT rizikos valdymo sistemos sritimi – jomis nustatomi finansų sektoriaus subjektams taikytini specifiniai elementai pagal Reglamento (ES) 2022/2554 15 straipsnį ir sukuriama supaprastinta IRT rizikos valdymo sistema, skirta to reglamento 16 straipsnio 1 dalyje nurodytiems finansų sektoriaus subjektams. Siekiant užtikrinti įprastos ir supaprastintos IRT rizikos valdymo sistemų tarpusavio nuoseklumą ir atsižvelgiant į tai, kad šios nuostatos turėtų būti pradėtos taikyti vienu metu, jas dera įtraukti į vieną bendrą teisėkūros procedūra priimamą aktą;

(28) šis reglamentas grindžiamas techninių reguliavimo standartų projektais, kuriuos Komisijai pateikė Europos bankininkystės institucija, Europos draudimo ir profesinių pensijų institucija ir Europos vertybinių popierių ir rinkų institucija (Europos priežiūros institucijos), pasikonsultavusios su Europos Sąjungos kibernetinio saugumo agentūra (ENISA);

([3]) 2012 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 648/2012 dėl ne biržos išvestinių finansinių priemonių, pagrindinių sandorio šalių ir sandorių duomenų saugyklų (OL L 201, 2012 7 27, p. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) 2014 m. gegužės 15 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 600/2014 dėl finansinių priemonių rinkų, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 648/2012 (OL L 173, 2014 6 12, p. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 909/2014 dėl atsiskaitymo už vertybinius popierius gerinimo Europos Sąjungoje ir centrinių vertybinių popierių depozitoriumų, kuriuo iš dalies keičiamos direktyvos 98/26/EB ir 2014/65/ES bei Reglamentas (ES) Nr. 236/2012 (OL L 257, 2014 8 28, p. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(29) Europos priežiūros institucijų jungtinis komitetas, nurodytas Europos Parlamento ir Tarybos reglamento (ES) Nr. 1093/2010 ([6]) 54 straipsnyje, Europos Parlamento ir Tarybos reglamento (ES) Nr. 1094/2010 ([7]) 54 straipsnyje ir Europos Parlamento ir Tarybos reglamento (ES) Nr. 1095/2010 ([8]) 54 straipsnyje, surengė atviras viešas konsultacijas dėl techninių reguliavimo standartų projektų, kuriais pagrįstas šis reglamentas, išnagrinėjo galimas siūlomų standartų sąnaudas ir naudą ir paprašė, kad pagal Reglamento (ES) Nr. 1093/2010 37 straipsnį įsteigta Bankininkystės suinteresuotųjų subjektų grupė, pagal Reglamento (ES) Nr. 1094/2010 37 straipsnį įsteigta Draudimo ir perdraudimo suinteresuotųjų subjektų grupė ir Profesinių pensijų suinteresuotųjų subjektų grupė ir pagal Reglamento (ES) Nr. 1095/2010 37 straipsnį įsteigta Vertybinių popierių ir rinkų suinteresuotųjų subjektų grupė pateiktų rekomendacijų;

(30) jeigu pagal šiame akte nustatytus įpareigojimus turi būti tvarkomi asmens duomenys, reikėtų visapusiškai laikytis reglamentų (ES) 2016/679 ([9]) ir (ES) 2018/1725 ([10]). Pavyzdžiui, tais atvejais, kai asmens duomenys renkami siekiant užtikrinti tinkamą incidentų aptikimą, reikėtų laikytis duomenų kiekio mažinimo principo. Rengiant šio akto tekstą taip pat konsultuotasi su Europos duomenų apsaugos priežiūros pareigūnu,

PRIĖMĖ ŠĮ REGLAMENTĄ:

I ANTRAŠTINĖ DALIS

BENDRIEJI PRINCIPAI

1 straipsnis

Bendras rizikos profilis ir sudėtingumas

Rengiant ir įgyvendinant II antraštinėje dalyje nurodytą IRT saugumo politiką, procedūras, protokolus ir priemones ir III antraštinėje dalyje nurodytą supaprastintą IRT rizikos valdymo sistemą, atsižvelgiama į finansų sektoriaus subjekto dydį ir bendrą rizikos profilį, taip pat į jo paslaugų, veiklos ir operacijų pobūdį, mastą ir didesnio ar mažesnio sudėtingumo elementus, įskaitant elementus, susijusius su:

a) šifravimu ir kriptografija;

b) IRT operacijų saugumu;

c) tinklo saugumu;

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1094/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos draudimo ir profesinių pensijų institucija), iš dalies keičiamas Sprendimas Nr. 716/2009/EB ir panaikinamas Komisijos sprendimas 2009/79/EB (OL L 331, 2010 12 15, p. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB (OL L 331, 2010 12 15, p. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) IRT projektų ir pakeitimų valdymu;

e) galimu IRT rizikos poveikiu duomenų konfidencialumui, vientisumui ir prieinamumui ir galimu sutrikimų poveikiu finansų sektoriaus subjekto veiklos tęstinumui ir prieinamumui.

II ANTRAŠTINĖ DALIS

TOLESNIS IRT RIZIKOS VALDYMO PRIEMONIŲ, METODŲ, PROCESŲ IR POLITIKOS DERINIMAS PAGAL REGLAMENTO (ES) 2022/2554 15 STRAIPSNĮ

I SKYRIUS

IRT SAUGUMO POLITIKA, PROCEDŪROS, PROTOKOLAI IR PRIEMONĖS

1 SKIRSNIS

2 straipsnis

Bendrieji IRT saugumo politikos, procedūrų, protokolų ir priemonių elementai

1. Finansų sektoriaus subjektai užtikrina, kad jų IRT saugumo politika, informacijos saugumo ir susijusios procedūros, protokolai ir priemonės, nurodyti Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje, būtų įtraukti į jų IRT rizikos valdymo sistemą. Finansų sektoriaus subjektai nustato savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus šiame skyriuje, siekdami:

a) užtikrinti tinklų saugumą;

b) pateikti tinkamas apsaugos nuo įsibrovimo ir neteisėto duomenų naudojimo priemones;

c) išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą, be kita ko, taikant kriptografinius metodus;

d) užtikrinti tikslų ir greitą duomenų perdavimą be didelių sutrikimų ir nepagrįsto vėlavimo.

2. Finansų sektoriaus subjektai užtikrina, kad 1 dalyje nurodyta jų IRT saugumo politika atitiktų šiuos reikalavimus:

a) būtų suderinta su finansų sektoriaus subjekto informacijos saugumo tikslais, įtrauktais į skaitmeninės veiklos atsparumo strategiją, nurodytą Reglamento (ES) 2022/2554 6 straipsnio 8 dalyje;

b) nurodytų datą, kurią valdymo organas oficialiai patvirtino IRT saugumo politiką;

c) apimtų rodiklius ir priemones:

i) IRT saugumo politikos, procedūrų, protokolų ir priemonių įgyvendinimui stebėti;

ii) to įgyvendinimo išimtims registruoti;

iii) finansų sektoriaus subjekto skaitmeninės veiklos atsparumui užtikrinti ii papunktyje nurodytų išimčių atveju;

d) būtų nustatytos visų lygmenų darbuotojų pareigos siekiant užtikrinti finansų sektoriaus subjekto IRT saugumą;

e) būtų nustatytos pasekmės, kurias patirtų IRT saugumo politikos nesilaikantys finansų sektoriaus subjekto darbuotojai, jei tokios paskirties nuostatos nenustatytos kita finansų sektoriaus subjekto politika;

f) būtų išvardyti atnaujintini dokumentai;

g) būtų nustatyta pareigų atskyrimo tvarka pagal trijų lygių kontrolės modelį arba kitą taikomą vidaus rizikos valdymo ir kontrolės modelį, kad būtų išvengta interesų konfliktų;

h) būtų atsižvelgta į pažangiausią praktiką ir atitinkamais atvejais į standartus, apibrėžtus Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte;

i) būtų nustatyti IRT saugumo politikos, procedūrų, protokolų ir priemonių kūrimo, įgyvendinimo ir priežiūros vaidmenys ir pareigos;

j) būtų peržiūrima pagal Reglamento (ES) 2022/2554 6 straipsnio 5 dalį;

k) būtų atsižvelgta į su finansų sektoriaus subjektu susijusius esminius pokyčius, be kita ko, finansų sektoriaus subjekto veiklos ar procesų, kibernetinių grėsmių aplinkos ar taikomų teisinių įpareigojimų esminius pokyčius.

2 SKIRSNIS

3 straipsnis

IRT rizikos valdymas

Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT rizikos valdymo politiką ir procedūras, apimančias visus šiuos elementus:

a) nuorodą į patvirtintą priimtiną IRT rizikos lygį, nustatytą pagal Reglamento (ES) 2022/2554 6 straipsnio 8 dalies b punktą;

b) IRT rizikos vertinimo procedūrą ir metodiką, kuriose nustatomi:

   i) pažeidžiamumai ir grėsmės, darantys ar galintys daryti poveikį palaikomoms veiklos funkcijoms, šias funkcijas palaikančioms IRT sistemoms ir IRT turtui;

   ii) kiekybiniai ar kokybiniai rodikliai, pagal kuriuos vertinamas poveikis ir i punkte nurodytų pažeidžiamumų ir grėsmių tikimybė;

c) procedūrą, pagal kurią identifikuojamos, įgyvendinamos ir dokumentuojamos veiksmų su IRT rizika priemonės, taikomos identifikuotai ir įvertintai IRT rizikai, įskaitant veiksmų su IRT rizika priemones, kurios yra būtinos, kad IRT rizika neviršytų a punkte nurodytos priimtinos rizikos lygio;

d) dėl liekamosios IRT rizikos, kuri vis dar kyla įgyvendinus c punkte nurodytas veiksmų su IRT rizika priemones:

   i) tos liekamosios IRT rizikos identifikavimo nuostatas;

   ii) priskirtus vaidmenis ir pareigas, susijusius su:

      (1) liekamosios IRT rizikos, viršijančios finansų sektoriaus subjekto priimtinos rizikos lygį, nurodytą a punkte, pripažinimu;

      (2) peržiūros procesu, nurodytu šio d punkto iv papunktyje;

   iii) pripažintos liekamosios IRT rizikos aprašo, be kita ko, nurodant tos rizikos priėmimo pagrindimą, parengimą;

   iv) pripažintos liekamosios IRT rizikos peržiūros bent kartą per metus nuostatas, įskaitant:

      1. bet kokių liekamosios IRT rizikos pokyčių nustatymą;

      2. turimų poveikio mažinimo priemonių vertinimą;

      3. vertinimą, ar liekamosios IRT rizikos pripažinimą pagrindžiančios priežastys vis dar aktualios ir egzistuoja peržiūros metu;

e) nuostatas dėl stebėsenos, susijusios su:

   i) visais IRT rizikos ir kibernetinių grėsmių aplinkos pokyčiais;

   ii) vidaus ir išorės pažeidžiamumais ir grėsmėmis;

   iii) finansų sektoriaus subjekto IRT rizika, kai ta stebėsena sudaro sąlygas greitai aptikti pokyčius, galinčius daryti poveikį subjekto IRT rizikos profiliui;

f) nuostatas dėl proceso, kuriuo užtikrinama, kad būtų atsižvelgta į visus finansų sektoriaus subjekto veiklos strategijos ir skaitmeninės veiklos atsparumo strategijos pokyčius.

Taikant pirmos pastraipos c punktą, tame punkte nurodyta procedūra užtikrinama:

a) įgyvendinamų veiksmų su IRT rizika priemonių veiksmingumo stebėsena;

b) įvertinimas, ar neviršijamas nustatytas finansų sektoriaus subjekto priimtinos rizikos lygis;

c) įvertinimas, ar finansų sektoriaus subjektas ėmėsi veiksmų, kad prireikus tas priemones pakoreguotų ar patobulintų.

3 SKIRSNIS

IRT TURTO VALDYMAS

4 straipsnis

IRT turto valdymo politika

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT turto valdymo politiką ir įtraukia ją į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje.

2. 1 dalyje nurodyta ICT turto valdymo politika:

a) nurodoma vykdyti pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį identifikuoto ir suklasifikuoto IRT turto stebėseną ir valdymą per gyvavimo ciklą;

b) finansų sektoriaus subjektas įpareigojamas registruoti visą šią informaciją:

i) kiekvieno IRT turto objekto unikalų identifikatorių;

ii) informaciją apie fizinę arba loginę kiekvieno IRT turto objekto vietą;

iii) viso IRT turto klasifikaciją, kaip nurodyta Reglamento (ES) 2022/2554 8 straipsnio 1 dalyje;

iv) IRT turto savininkų tapatybes;

v) IRT turto palaikomas veiklos funkcijas ar paslaugas;

vi) IRT veiklos tęstinumo reikalavimus, įskaitant veiklos atkūrimo laiko ir veiklos atkūrimo taško tikslus;

vii) tai, ar IRT turtas gali būti arba yra pasiekiamas per išorės tinklus, įskaitant internetą;

viii) IRT turto ir veiklos funkcijų, kurioms naudojamas tas IRT turtas, sąsajas ir tarpusavio priklausomybę;

ix) atitinkamais atvejais šią informaciją apie kiekvieną IRT turto objektą – IRT paslaugas teikiančios trečiosios šalies vykdomo įprastų, išplėstinių ir pritaikytųjų palaikymo paslaugų teikimo pabaigos datas, po kurių jo tiekėjas ar IRT paslaugas teikianti trečioji šalis to IRT turto nebepalaikys;

c) finansų sektoriaus subjektai, išskyrus labai mažas įmones, įpareigojami registruoti informaciją, reikalingą Reglamento (ES) 2022/2554 8 straipsnio 7 dalyje nurodytam specialiam visų senųjų IRT sistemų IRT rizikos vertinimui atlikti.

5 straipsnis

IRT turto valdymo procedūra

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT turto valdymo procedūrą.

2. 1 dalyje nurodytoje IRT turto valdymo procedūroje nustatomi informacinio turto ir IRT turto, kuriuo palaikomos veiklos funkcijos, ypatingos svarbos vertinimo kriterijai. Atliekant tą vertinimą atsižvelgiama į:

a) su tomis veiklos funkcijomis susijusią IRT riziką ir jų priklausomybę nuo informacinio turto ar IRT turto;

b) poveikį, kurį informacinio turto ar IRT turto duomenų konfidencialumo, vientisumo ir prieinamumo praradimas padarytų finansų sektoriaus subjektų veiklos procesams ir veiklai.

4 SKIRSNIS

ŠIFRAVIMAS IR KRIPTOGRAFIJA

6 straipsnis

Šifravimas ir kriptografinės kontrolės priemonės

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina šifravimo ir kriptografinės kontrolės priemonių politiką ir įtraukia ją į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje.

2. Finansų sektoriaus subjektai 1 dalyje nurodytą šifravimo ir kriptografinės kontrolės priemonių politiką rengia remdamiesi patvirtintų duomenų klasifikavimo ir IRT rizikos vertinimo procesų rezultatais. Toje politikoje pateikiamos taisyklės, kuriomis reglamentuojami visi šie elementai:

a) saugomų ir perduodamų duomenų užšifravimas;

b) naudojamų duomenų užšifravimas, kai reikia;

c) vidaus tinklų ryšių ir duomenų, kuriais keičiamasi su išorės šalimis, užšifravimas;

d) 7 straipsnyje nurodytas kriptografinių raktų valdymas nustatant kriptografinių raktų teisingo naudojimo, apsaugos ir gyvavimo ciklo taisykles.

Taikant b punktą, tais atvejais, kai užšifruoti naudojamų duomenų neįmanoma, finansų sektoriaus subjektai tvarko naudojamus duomenis atskirtoje, apsaugotoje aplinkoje arba imasi lygiaverčių priemonių, kad užtikrintų duomenų konfidencialumą, vientisumą, autentiškumą ir prieinamumą.

3. Finansų sektoriaus subjektai, atsižvelgdami į pažangiausią praktiką ir Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte apibrėžtus standartus, į 1 dalyje nurodytą šifravimo ir kriptografinės kontrolės priemonių politiką įtraukia kriptografinių metodų ir naudojimo praktikos atrankos kriterijus ir atitinkamo IRT turto klasifikaciją, nustatytą pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį. Finansų sektoriaus subjektai, kurie negali laikytis pažangiausios praktikos ar standartų arba taikyti pačių patikimiausių metodų, priima poveikio mažinimo ir stebėsenos priemones, kuriomis užtikrina atsparumą kibernetinėms grėsmėms.

4. Finansų sektoriaus subjektai į 1 dalyje nurodytą šifravimo ir kriptografinės kontrolės priemonių politiką įtraukia nuostatas dėl reikiamo kriptografinės technologijos naujinimo ar keitimo remiantis kriptoanalizės patobulinimais. Tais naujiniais ar keitiniais užtikrinama, kad kriptografinė technologija išliktų atspari kibernetinėms grėsmėms, kaip reikalaujama 10 straipsnio 2 dalies a punktu. Finansų sektoriaus subjektai, kurie negali atnaujinti ar pakeisti kriptografinės technologijos, priima poveikio mažinimo ir stebėsenos priemones, kuriomis užtikrina atsparumą kibernetinėms grėsmėms.

5. Finansų sektoriaus subjektai į 1 dalyje nurodytą šifravimo ir kriptografinės kontrolės priemonių politiką įtraukia reikalavimą registruoti poveikio mažinimo ir stebėsenos priemonių priėmimą, kai jos priimamos pagal 3 ir 4 dalis, ir pateikti motyvuotą to priėmimo paaiškinimą.

7 straipsnis

Kriptografinių raktų valdymas

1. Finansų sektoriaus subjektai į 6 straipsnio 2 dalies d punkte nurodytą kriptografinių raktų valdymo politiką įtraukia reikalavimus dėl kriptografinių raktų valdymo visą jų gyvavimo ciklą, be kita ko, dėl tų kriptografinių raktų kūrimo, atnaujinimo, saugojimo, jų atsarginių kopijų kūrimo, archyvavimo, gavimo, persiuntimo, pašalinimo, panaikinimo ir sunaikinimo.

2. Finansų sektoriaus subjektai nustato ir įgyvendina kontrolės priemones kriptografiniams raktams apsaugoti nuo praradimo, neteisėtos prieigos, atskleidimo ir pakeitimo visą jų gyvavimo ciklą. Finansų sektoriaus subjektai tas kontrolės priemones kuria remdamiesi patvirtintų duomenų klasifikavimo ir IRT rizikos vertinimo procesų rezultatais.

3. Finansų sektoriaus subjektai rengia ir taiko metodus, pagal kuriuos kriptografiniai raktai pakeičiami, jei jie būtų prarasti, būtų pažeistas jų saugumas arba jie būtų sugadinti.

4. Finansų sektoriaus subjektai sukuria ir prižiūri bent IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, visų sertifikatų ir jų saugojimo įrenginių registrą. Finansų sektoriaus subjektai tą registrą atnaujina.

5. Finansų sektoriaus subjektai užtikrina punktualų sertifikatų atnaujinimą prieš pasibaigiant jų galiojimui.

5 SKIRSNIS

IRT OPERACIJŲ SAUGUMAS

8 straipsnis

IRT operacijų politika ir procedūros

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT operacijų valdymo procedūras ir įtraukia jas į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje. Ta politika ir procedūromis nustatoma, kaip finansų sektoriaus subjektai valdo, stebi, kontroliuoja ir atkuria savo IRT turtą ir, be kita ko, dokumentuoja IRT operacijas.

2. 1 dalyje nurodyta IRT operacijų politika ir procedūros apima visus šiuos elementus:

a) IRT turto aprašymą, apimantį visus šiuos elementus:

   i) saugaus IRT sistemos diegimo, priežiūros, konfigūravimo ir išinstaliavimo reikalavimus;

   ii) informacinio turto, kurį naudoja IRT turtas, valdymo reikalavimus, įskaitant to informacinio turto automatinio ir rankinio apdorojimo ir tvarkymo reikalavimus;

   iii) senųjų IRT sistemų nustatymo ir kontrolės reikalavimus;

(b) IRT sistemų kontrolės ir stebėsenos reikalavimus, apimančius visus šiuos elementus:

   i) IRT sistemų atsarginių kopijų kūrimo ir atkūrimo reikalavimus;

   ii) chronologijos reikalavimus atsižvelgiant į IRT sistemų tarpusavio priklausomybę;

   iii) audito sekos ir sistemos registracijos žurnalų informacijos protokolus;

   iv) reikalavimus, kuriais užtikrinama, kad atliekant vidaus auditą ir kitokį testavimą būtų kuo labiau sumažinama veiklos operacijų sutrikimų tikimybė;

   v) reikalavimus, pagal kuriuos IRT produkcinė aplinka atskiriama nuo kūrimo, testavimo ar kitokios neprodukcinės aplinkos;

   vi) reikalavimus kūrimo ir testavimo užduotis vykdyti nuo produkcinės aplinkos atskirtose aplinkose;

   vii) reikalavimus kūrimo ir testavimo užduotis vykdyti produkcinėse aplinkose;

c) IRT sistemų klaidų valdymą, apimantį visus šiuos elementus:

i) klaidų valdymo procedūras ir protokolus;

ii) aptarnavimo ir incidentų sprendimo kontaktinius duomenis, įskaitant išorės aptarnavimo kontaktinius duomenis tam atvejui, jei kiltų nenumatytų operacinių ar techninių problemų;

iii) IRT sistemos paleidimo iš naujo, ankstesnės būklės atkūrimo ir veiklos atkūrimo procedūras, taikytinas IRT sistemos sutrikimo atveju.

Taikant b punkto v papunktį, atskyrimas apima visus aplinkos komponentus, įskaitant paskyras, duomenis ir jungtis, kaip reikalaujama pagal 13 straipsnio pirmos pastraipos a punktą.

Taikant b punkto vii papunktį, 1 dalyje nurodytoje politikoje ir procedūrose turėtų būti nustatyta, kad atvejai, kai testavimas atliekamas produkcinėje aplinkoje, turi būti aiškiai nustatyti, pagrįsti ir ribotos trukmės, taip pat juos turi patvirtinti atitinkamas funkcijas pagal 16 straipsnio 6 dalį einantis darbuotojas. Kūrimo ir testavimo veiklos produkcinėje aplinkoje metu finansų sektoriaus subjektai užtikrina IRT sistemų ir produkcinės aplinkos duomenų prieinamumą, konfidencialumą, vientisumą ir autentiškumą.

9 straipsnis

Pajėgumo ir veiklos rezultatų valdymas

1. Finansų sektoriaus subjektai parengia, dokumentuoja, įgyvendina ir į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje, įtraukia pajėgumo ir veiklos rezultatų valdymo procedūras, taikytinas:

a) nustatant jų IRT sistemų pajėgumo reikalavimus;

b) vykdant išteklių optimizavimą;

c) stebėsenos procedūroms, kuriomis siekiama palaikyti ir gerinti:

i) duomenų ir IRT sistemų prieinamumą;

ii) IRT sistemų veiksmingumą;

iii) IRT pajėgumo trūkumo prevenciją.

2. 1 dalyje nurodytomis pajėgumo ir veiklos rezultatų valdymo procedūromis užtikrinama, kad finansų sektoriaus subjektai imtųsi tinkamų priemonių, kad atsižvelgtų į IRT sistemų, kurioms taikomi ilgai trunkantys ar sudėtingi viešųjų pirkimų ar patvirtinimo procesai arba kurios naudoja daug išteklių, ypatumus.

10 straipsnis

Pažeidžiamumų ir pataisų valdymas

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina pažeidžiamumų valdymo procedūras ir įtraukia jas į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje.

2. Taikant 1 dalyje nurodytas pažeidžiamumų valdymo procedūras:

a) nustatomi ir atnaujinami aktualūs ir patikimi informacijos šaltiniai, padedantys plėsti ir atnaujinti žinias apie pažeidžiamumus;

b) užtikrinamas automatinis IRT turto pažeidžiamumų skenavimas ir vertinimas, o tos veiklos periodiškumas ir mastas turi būti proporcingi klasifikacijai pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir bendram IRT turto rizikos profiliui;

c) tikrinama, ar:

i) IRT paslaugas teikiančios trečiosios šalys valdo pažeidžiamumus, susijusius su finansų sektoriaus subjektui teikiamomis IRT paslaugomis;

ii) tie paslaugų teikėjai laiku praneša finansų sektoriaus subjektui bent kritinius pažeidžiamumus ir statistinius duomenis bei tendencijas;

d) stebima, kaip naudojamos:

i) trečiųjų šalių bibliotekos, įskaitant atvirojo kodo bibliotekas, naudojamos IRT paslaugoms, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos;

ii) IRT paslaugos, kurias sukūrė pats finansų sektoriaus subjektas arba kurias konkrečiai jam pritaikė ar sukūrė IRT paslaugas teikianti trečioji šalis;

e) nustatomos atsakingo informacijos apie pažeidžiamumus atskleidimo klientams, sandorio šalims ir visuomenei procedūros;

f) šalinant aptiktus pažeidžiamumus pirmenybė teikiama pataisų diegimui ir kitoms poveikio mažinimo priemonėms;

g) stebimas ir tikrinamas pažeidžiamumų koregavimas;

h) reikalaujama registruoti visus aptiktus pažeidžiamumus, darančius poveikį IRT sistemai, ir stebėti jų pašalinimą.

Taikydami b punktą, finansų sektoriaus subjektai automatinį IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, pažeidžiamumų skenavimą ir vertinimą atlieka bent kartą per savaitę.

Taikydami c punktą, finansų sektoriaus subjektai teikia prašymą IRT paslaugas teikiančioms trečiosioms šalims išnagrinėti atitinkamus pažeidžiamumus, nustatyti pagrindines priežastis ir įgyvendinti tinkamus poveikio mažinimo veiksmus.

Taikydami d punktą, finansų sektoriaus subjektai, atitinkamais atvejais bendradarbiaudami su IRT paslaugas teikiančiomis trečiosiomis šalimis, stebi trečiųjų šalių bibliotekų versijas ir galimus naujinius. Parengto naudoti IRT turto ar IRT turto, įsigyto ir naudojamo teikti IRT paslaugoms, kuriomis nepalaikomos ypatingos svarbos arba svarbios funkcijos, komponentų atveju finansų sektoriaus subjektai kuo įdėmiau stebi trečiųjų šalių bibliotekų, įskaitant atvirojo kodo bibliotekas, naudojimą.

Taikydami f punktą, finansų sektoriaus subjektai įvertina IRT turto, kuriam daro poveikį aptikti pažeidžiamumai, pažeidžiamumo kritiškumą, klasifikaciją pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir rizikos profilį.

3. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina pataisų valdymo procedūras ir įtraukia jas į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje.

4. Taikant 3 dalyje nurodytas pataisų valdymo procedūras:

a) kuo tiksliau automatizuotomis priemonėmis identifikuojamos ir įvertinamos programinės ir aparatinės įrangos pataisos ir naujiniai, kurie yra prieinami;

b) nustatomos skubaus IRT turto pataisų diegimo ir naujinimo procedūros;

c) testuojamos ir diegiamos programinės ir aparatinės įrangos pataisos ir naujiniai pagal 8 straipsnio 2 dalies b punkto v, vi ir vii papunkčius;

d) nustatomi programinės ir aparatinės įrangos pataisų ir naujinių diegimo terminai ir incidentų sprendimo procedūros tiems atvejams, kai terminų laikytis neįmanoma.

11 straipsnis

Duomenų ir sistemų apsauga

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina duomenų ir sistemų apsaugos procedūrą ir įtraukia ją į savo IRT saugumo politiką, procedūras, protokolus ir priemones, nurodytus Reglamento (ES) 2022/2554 9 straipsnio 2 dalyje.

2. 1 dalyje nurodyta duomenų ir sistemų apsaugos procedūra apima visus toliau nurodytus elementus, susijusius su duomenų ir IRT sistemų apsauga, pagal klasifikaciją pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį:

a) šio reglamento 21 straipsnyje nurodytus prieigos apribojimus, papildančius kiekvieno klasifikacijos lygio apsaugos reikalavimus;

b) IRT turto saugios bazinės konfigūracijos, kuria kuo labiau sumažinama tam IRT turtui kylanti kibernetinė grėsmė, ir priemonių tų bazinių konfigūracijų veiksmingam diegimui reguliariai patikrinti nustatymą;

c) apsaugos priemonių, kuriomis užtikrinama, kad IRT sistemose ir galiniuose įrenginiuose būtų diegiama tik leidžiama programinė įranga, nustatymą;

d) apsaugos nuo kenkėjiškų kodų priemonių nustatymą;

e) apsaugos priemonių, kuriomis užtikrinama, kad finansų sektoriaus subjekto duomenims persiųsti ir saugoti būtų naudojamos tik leidžiamos duomenų saugojimo laikmenos, sistemos ir galiniai įrenginiai, nustatymą;

f) šiuos reikalavimus, kuriais užtikrinamas saugus nešiojamųjų galinių įrenginių ir privačių stacionarių galinių įrenginių naudojimas:

   i) reikalavimą taikyti valdymo sprendimą, kuriuo nuotoliniu būdu valdomi galiniai įrenginiai ir nuotoliniu būdu ištrinami finansų sektoriaus subjekto duomenys;

   ii) reikalavimą taikyti saugumo mechanizmus, kurių darbuotojai ar IRT paslaugas teikiančios trečiosios šalys negali neteisėtai pakeisti, pašalinti ar apeiti;

   iii) reikalavimą naudoti prijungiamus duomenų saugojimo įrenginius tik tuo atveju, kai liekamoji IRT rizika neviršija finansų sektoriaus subjekto priimtinos rizikos lygio, nurodyto 3 straipsnio pirmos pastraipos a punkte;

g) finansų sektoriaus subjekto patalpose laikomų ar išorėje saugomų duomenų, kurių finansų sektoriaus subjektui nebereikia rinkti ar saugoti, saugaus ištrynimo procesą;

h) finansų sektoriaus subjekto patalpose laikomų ar išorėje saugomų duomenų saugojimo įrenginių, kuriuose įrašyta konfidenciali informacija, saugaus sunaikinimo procesą;

i) sistemų ir galinių įrenginių apsaugos nuo duomenų praradimo ir nutekinimo priemonių nustatymą ir įgyvendinimą;

j) apsaugos priemonių, kuriomis užtikrinama, kad nuotolinis darbas ir privačių galinių įrenginių naudojimas nedarytų neigiamo poveikio finansų sektoriaus subjekto IRT saugumui, įgyvendinimą;

k) reikalavimų išlaikyti IRT paslaugas teikiančios trečiosios šalies naudojamo IRT turto ar paslaugų skaitmeninės veiklos atsparumą, remiantis duomenų klasifikavimo ir IRT rizikos vertinimo rezultatais, nustatymą ir įgyvendinimą.

Taikant b punktą, nustatant tame punkte nurodytą saugią bazinę konfigūraciją atsižvelgiama į pažangiausią praktiką ir tinkamus metodus, išdėstytus Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte apibrėžtuose standartuose.

Taikant k punktą, finansų sektoriaus subjektai atsižvelgia į:

a) pardavėjo rekomenduotų nuostačių taikymą elementams, kuriuos valdo finansų sektoriaus subjektas;

b) aiškų informacijos saugumo užtikrinimo vaidmenų ir pareigų paskirstymą tarp finansų sektoriaus subjekto ir IRT paslaugas teikiančios trečiosios šalies pagal Reglamento (ES) 2022/2554 28 straipsnio 1 dalies a punkte nurodytą principą, pagal kurį visa atsakomybė tenka finansų sektoriaus subjektui, o ne IRT paslaugas teikiančiai trečiajai šaliai, ir jų paskirstymą to reglamento 28 straipsnio 2 dalyje nurodytiems finansų sektoriaus subjektams pagal finansų sektoriaus subjekto IRT paslaugų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, naudojimo politiką;

c) poreikį užtikrinti ir išlaikyti tinkamą finansų sektoriaus subjekto kompetenciją naudojamos paslaugos valdymo ir saugumo srityse;

d) technines ir organizacines priemones, kuriomis kuo labiau sumažinama rizika, susijusi su infrastruktūra, kurią IRT paslaugas teikianti trečioji šalis naudoja savo IRT paslaugoms teikti, atsižvelgiant į pažangiausią praktiką ir Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte apibrėžtus standartus.

12 straipsnis

Registravimas

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina registravimo procedūras, protokolus ir priemones ir įtraukia juos į apsaugos nuo įsibrovimo ir neteisėto duomenų naudojimo priemones.

2. 1 dalyje nurodytos registravimo procedūros, protokolai ir priemonės apima visus šiuos elementus:

a) registruotinų įvykių nustatymą, registracijos žurnalų saugojimo laikotarpį ir priemones registracijos žurnalų duomenims apsaugoti ir tvarkyti, atsižvelgiant į paskirtį, dėl kurios registracijos žurnalai buvo sukurti;

b) registracijos žurnalų detalumo lygio suderinimą su jų paskirtimi ir naudojimu, kad būtų lengviau veiksmingai aptikti neįprastą veiklą, kaip nurodyta 24 straipsnyje;

c) reikalavimą registruoti įvykius, susijusius su:

   i) loginės ir fizinės prieigos kontrole, nurodyta 21 straipsnyje, ir tapatybės duomenų tvarkymu;

   ii) pajėgumų valdymu;

   iii) pakeitimų valdymu;

   iv) IRT operacijomis, įskaitant IRT sistemos veiklą;

   v) tinklo duomenų srauto veiklą, įskaitant IRT tinklo veikimą;

d) priemones registravimo sistemoms ir registracijos žurnalų informacijai apsaugoti nuo neteisėto keitimo, pašalinimo ir neteisėtos prieigos saugojimo, perdavimo ir prireikus naudojimo metu;

e) priemones registravimo sistemų gedimui aptikti;

f) (nedarant poveikio jokiems taikytiniems reguliavimo reikalavimams pagal Sąjungos ar nacionalinę teisę) visų finansų sektoriaus subjekto IRT sistemų laikrodžių sinchronizavimą pagal dokumentuotą patikimą atskaitinio laiko šaltinį.

Taikydami a punktą, finansų sektoriaus subjektai nustato saugojimo laikotarpį atsižvelgdami į veiklos ir informacijos saugumo tikslus, įvykio registravimo registracijos žurnaluose priežastį ir IRT rizikos vertinimo rezultatus.

6 skirsnis

Tinklo saugumas

13 straipsnis

Tinklo saugumo valdymas

Finansų sektoriaus subjektai parengia, dokumentuoja, įgyvendina ir į savo tinklo apsaugos nuo įsibrovimo ir netinkamo duomenų naudojimo priemones įtraukia tinklo saugumo valdymo politiką, procedūras, protokolus ir priemones, apimančias visus šiuos elementus:

a) IRT sistemų ir tinklų atskyrimą ir segmentavimą atsižvelgiant į:

   i) funkcijų, kurios palaikomos tomis IRT sistemomis ir tinklais, ypatingą svarbą ar svarbumą;

   ii) klasifikaciją pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį;

   iii) bendrą IRT turto, kuris naudojasi tomis IRT sistemomis ir tinklais, rizikos profilį;

b) visų finansų sektoriaus subjekto tinklų ryšių ir duomenų srautų dokumentavimą;

c) atskiro skirtojo tinklo naudojimą IRT turtui administruoti;

d) tinklo prieigos kontrolės nustatymą ir įgyvendinimą siekiant neleisti prie finansų sektoriaus subjekto tinklo jungtis neturinčiam leidimo įrenginiui ar sistemai arba galiniam įrenginiui, neatitinkančiam finansų sektoriaus subjekto saugumo reikalavimų, ir aptikti tokio jungimosi atvejus;

e) tinklų ryšių, vykdomų per įmonių tinklus, viešuosius tinklus, namų ūkių tinklus, trečiųjų šalių tinklus ir belaidžius tinklus, užšifravimą, ryšių protokolų užšifravimą, atsižvelgiant į patvirtinto duomenų klasifikavimo rezultatus, IRT rizikos vertinimo rezultatus ir 6 straipsnio 2 dalyje nurodytų tinklų ryšių užšifravimą;

f) tinklų projektavimą pagal finansų sektoriaus subjekto nustatytus IRT saugumo reikalavimus, atsižvelgiant į pažangiausią praktiką, kad būtų užtikrintas tinklo konfidencialumas, vientisumas ir prieinamumas;

g) tinklo duomenų srauto tarp vidaus tinklų ir interneto bei kitų išorės jungčių saugumo užtikrinimą;

h) užkardos taisyklių ir ryšių filtrų nustatymo, įgyvendinimo, patvirtinimo, pakeitimo ir peržiūros vaidmenų, pareigų ir etapų nustatymą;

i) tinklo architektūros ir tinklo saugumo projekto peržiūrų atlikimą kartą per metus, o labai mažų įmonių – reguliariais intervalais, siekiant identifikuoti galimus pažeidžiamumus;

j) priemones potinkliams ir tinklo komponentams bei įrenginiams prireikus laikinai izoliuoti;

k) visų tinklo komponentų saugios bazinės konfigūracijos įgyvendinimą ir tinklo bei tinklo įrenginių atsparumo didinimą pagal pardavėjo nurodymus, taikytinus standartus, apibrėžtus Reglamento (ES) Nr. 1025/2012 2 straipsnio 1 punkte, ir pažangiausią praktiką;

l) procedūras, pagal kurias po nurodyto neaktyvumo laikotarpio sistemos ir nuotoliniai seansai apribojami, užrakinami ir nutraukiami;

m) dėl tinklo paslaugų susitarimų:

   i) IRT ir informacijos saugumo priemonių, paslaugų lygių ir valdymo reikalavimų, taikomų visoms tinklo paslaugoms, nustatymą ir specifikacijas;

   ii) tai, ar tas paslaugas tiekia grupės vidaus IRT paslaugų teikėjas, ar IRT paslaugas teikiančios trečiosios šalys.

Taikydami h punktą, finansų sektoriaus subjektai reguliariai peržiūri užkardos taisykles ir ryšių filtrus pagal susijusių IRT sistemų klasifikaciją pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir bendrą IRT turto rizikos profilį. Finansų sektoriaus subjektai tikrina IRT sistemoms, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, taikomų užkardos taisyklių ir ryšių filtrų tinkamumą bent kas šešis mėnesius.

14 straipsnis

Perduodamos informacijos saugumo užtikrinimas

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina perduodamos informacijos apsaugos politiką, procedūras, protokolus ir priemones ir įtraukia juos į apsaugos priemones, kuriomis siekiama išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą. Visų pirma finansų sektoriaus subjektai užtikrina visus šiuos elementus:

a) tinklu perduodamų duomenų prieinamumą, autentiškumą, vientisumą bei konfidencialumą ir procedūrų, pagal kurias įvertinamas tų reikalavimų laikymasis, nustatymą;

b) duomenų nutekinimo prevenciją ir aptikimą ir saugų informacijos perdavimą tarp finansų sektoriaus subjekto ir išorės šalių;

c) konfidencialumo reikalavimų ar informacijos neatskleidimo susitarimų, atitinkančių finansų sektoriaus subjekto poreikius apsaugoti informaciją, susijusius tiek su finansų sektoriaus subjekto darbuotojais, tiek su trečiosiomis šalimis, įgyvendinimą, dokumentavimą ir reguliarią peržiūrą.

2. Finansų sektoriaus subjektai 1 dalyje nurodytą perduodamos informacijos apsaugos politiką, procedūras, protokolus ir priemones rengia remdamiesi patvirtintų duomenų klasifikavimo ir IRT rizikos vertinimo procesų rezultatais.

7 SKIRSNIS

IRT projektų ir pakeitimų valdymas

15 straipsnis

IRT projektų valdymas

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT projektų valdymo politiką ir įtraukia ją į apsaugos priemones, kuriomis siekiama išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą.

2. 1 dalyje nurodyta IRT projektų valdymo politika nustatomi elementai, kuriais užtikrinamas veiksmingas IRT projektų, susijusių su finansų sektoriaus subjekto IRT sistemų įsigijimu, priežiūra ir atitinkamais atvejais kūrimu, valdymas.

3. 1 dalyje nurodytoje IRT projektų valdymo politikoje nurodomi visi šie elementai:

a) IRT projektų tikslai;

b) IRT projektų valdymas, įskaitant vaidmenis ir pareigas;

c) IRT projektų planavimas, terminai ir etapai;

d) IRT projektų rizikos vertinimas;

e) atitinkamos tarpinės reikšmės;

f) pakeitimų valdymo reikalavimai;

g) visų reikalavimų, įskaitant saugumo reikalavimus, testavimas ir atitinkamas patvirtinimo procesas, taikomas diegiant IRT sistemą produkcinėje aplinkoje.

4. 1 dalyje nurodyta IRT projektų valdymo politika saugus IRT projektų įgyvendinimas užtikrinamas teikiant veiklos srities ar funkcijų, kurioms daro poveikį IRT projektas, būtiną informaciją ir ekspertines žinias.

5. Pagal 3 dalies d punkte nurodytą IRT projektų rizikos vertinimą 1 dalyje nurodyta IRT projektų valdymo politika nustatoma, kad apie IRT projektų, kuriais daromas poveikis ypatingos svarbos arba svarbioms finansų sektoriaus subjekto funkcijoms, nustatymą ir eigą, taip pat apie susijusią jų riziką būtų pranešama valdymo organui taip:

a) individualiai arba apibendrintai, priklausomai nuo IRT projektų svarbumo ir dydžio;

b) periodiškai ir prireikus, įvykus konkrečiam įvykiui.

16 straipsnis

IRT sistemų įsigijimas, kūrimas ir priežiūra

1. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT sistemų įsigijimo, kūrimo ir priežiūros politiką ir įtraukia ją į apsaugos priemones, kuriomis siekiama išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą. Pagal tą politiką:

a) nustatoma saugumo praktika ir metodika, susijusios su IRT sistemų įsigijimu, kūrimu ir priežiūra;

b) reikalaujama nustatyti:

   i) technines specifikacijas ir IRT technines specifikacijas, apibrėžtas Reglamento (ES) Nr. 1025/2012 2 straipsnio 4 ir 5 punktuose;

   ii) su IRT sistemų įsigijimu, kūrimu ir priežiūra susijusius reikalavimus, kuriais ypatingas dėmesys skiriamas IRT saugumo reikalavimams ir jų patvirtinimui, kurį atlieka atitinkamą veiklos funkciją vykdantis darbuotojas ir IRT turto savininkas pagal finansų sektoriaus subjekto vidaus valdymo priemones;

c) nustatomos priemonės, kuriomis mažinama netyčinio IRT sistemų pakeitimo ar tyčinio manipuliavimo jomis rizika tų IRT sistemų kūrimo, priežiūros ir diegimo produkcinėje aplinkoje metu.

2. Finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT sistemų įsigijimo, kūrimo ir priežiūros procedūrą, skirtą visų IRT sistemų testavimui ir patvirtinimui iki pradedant jas naudoti ir po priežiūros pagal 8 straipsnio 2 dalies b punkto v, vi ir vii papunkčius. Testavimo lygis turi būti proporcingas atitinkamų veiklos procedūrų ir IRT turto ypatingai svarbai. Testavimas turi būti suplanuotas taip, kad būtų galima patikrinti naujų IRT sistemų pajėgumą veikti, kaip numatyta, įskaitant subjekto viduje sukurtos programinės įrangos kokybę.

Pagrindinės sandorių šalys, be pirmoje pastraipoje išdėstytų reikalavimų, į pirmoje pastraipoje nurodyto testavimo planavimą ir atlikimą, kai tinkama, įtraukia:

a) tarpuskaitos narius ir klientus;

b) sąveikias pagrindines sandorių šalis;

c) kitas suinteresuotąsias šalis.

Centriniai vertybinių popierių depozitoriumai, be pirmoje pastraipoje išdėstytų reikalavimų, į pirmoje pastraipoje nurodyto testavimo planavimą ir atlikimą, kai tinkama, įtraukia:

a) naudotojus;

b) ypatingos svarbos komunalinių paslaugų ir ypatingos svarbos paslaugų teikėjus;

c) kitus centrinius vertybinių popierių depozitoriumus;

d) kitas rinkos infrastruktūras;

e) visas kitas įstaigas, su kuriomis centrinių vertybinių popierių depozitoriumus, kaip nustatyta jų veiklos tęstinumo politikoje, sieja tarpusavio priklausomybės ryšiai.

3. Pagal 2 dalyje nurodytą procedūrą atliekamos pirminio kodo peržiūros, apimančios tiek statinį, tiek dinaminį testavimą. Tas testavimas apima internetu pasiekiamų sistemų ir taikomųjų programų saugumo testavimą pagal 8 straipsnio 2 dalies b punkto v, vi ir vii papunkčius. Finansų sektoriaus subjektai:

a) identifikuoja ir analizuoja pirminio kodo pažeidžiamumus ir anomalijas;

b) priima veiksmų planą, pagal kurį tie pažeidžiamumai ir anomalijos šalinami;

c) stebi to veiksmų plano įgyvendinimą.

4. Pagal 2 dalyje nurodytą procedūrą ne vėliau kaip integravimo etapu atliekamas programinės įrangos paketų saugumo testavimas pagal 8 straipsnio 2 dalies b punkto v, vi ir vii papunkčius.

5. Pagal 2 dalyje nurodytą procedūrą nustatoma, kad:

a) neprodukcinėse aplinkose būtų saugomi tik anoniminiai, pseudoniminiai ar atsitiktine tvarka surinkti produkcinės aplinkos duomenys;

b) finansų sektoriaus subjektai turi apsaugoti duomenų vientisumą ir konfidencialumą neprodukcinėje aplinkoje.

6. Nukrypstant nuo 5 dalies, pagal 2 dalyje nurodytą procedūrą gali būti nustatyta, kad produkcinės aplinkos duomenys būtų saugomi tik konkretiems testavimo atvejams, ribotus laikotarpius, gavus atitinkamas funkcijas vykdančio darbuotojo patvirtinimą ir pranešus apie tokius atvejus IRT rizikos valdymo funkciją vykdančiam darbuotojui.

7. Pagal 2 dalyje nurodytą procedūrą nustatomas kontrolės priemonių įgyvendinimas siekiant apsaugoti subjekto viduje sukurto arba IRT paslaugas teikiančios trečiosios šalies sukurto ir finansų sektoriaus subjektui pateikto IRT sistemų pirminio kodo vientisumą.

8. 2 dalyje nurodyta procedūra nustatoma, kad IRT paslaugas teikiančių trečiųjų šalių pateikta arba iš atvirojo kodo projektų gauta nuosavybinė programinė įranga ir, kai įmanoma, pirminis kodas prieš jų diegimą produkcinėje aplinkoje turi būti analizuojami ir testuojami pagal 3 dalį.

9. Taikant rizika grindžiamą požiūrį, šio straipsnio 1–8 dalys taip pat taikomos IRT sistemoms, kurias sukūrė ar valdo ne IRT funkciją vykdantys naudotojai.

17 straipsnis

IRT pakeitimų valdymas

1. Finansų sektoriaus subjektai į apsaugos priemones, kuriomis siekiama išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą, įtraukia IRT pakeitimų valdymo procedūras, nurodytas Reglamento (ES) 2022/2554 9 straipsnio 4 dalies e punkte, taikomas visiems programinės įrangos, aparatinės įrangos, aparatinės programinės įrangos komponentų, sistemos ar saugumo parametrų pakeitimams ir apimančias visus šiuos elementus:

a) patikrinimą, ar įvykdyti IRT saugumo reikalavimai;

b) mechanizmus, kuriais užtikrinamas pakeitimų tvirtinimo funkcijų ir pakeitimų užsakymo bei jų įgyvendinimo funkcijų nepriklausomumas;

c) aiškiai aprašytus vaidmenis ir pareigas, kuriais užtikrinama, kad:

   i) pakeitimai būtų įvardyti ir suplanuoti;

   ii) būtų suplanuotas tinkamas pereinamasis laikotarpis;

   iii) pakeitimai būtų testuojami ir finalizuojami kontroliuojamu būdu;

   iv) būtų vykdomas veiksmingas kokybės užtikrinimas;

d) informacijos apie pakeitimus dokumentavimą ir perdavimą, be kita ko, nurodant:

   i) pakeitimo paskirtį ir apimtį;

   ii) pakeitimo įgyvendinimo tvarkaraštį;

   iii) numatomus rezultatus;

e) atsarginių procedūrų ir pareigų nustatymą, be kita ko, nustatant procedūras ir pareigas, susijusias su pakeitimų diegimo nutraukimu ar atkūrimu tuo atveju, kai pakeitimų įgyvendinti nepavyksta;

f) procedūras, protokolus ir priemones, pagal kurias valdant neatidėliotinus pakeitimus nustatomos tinkamos apsaugos priemonės;

g) procedūras, pagal kurias dokumentuojami, pakartotinai įvertinami, vertinami ir patvirtinami neatidėliotini pakeitimai po jų įgyvendinimo, įskaitant aplinkinius sprendimus ir pataisas;

h) pakeitimo galimo poveikio taikomoms IRT apsaugos priemonėms nustatymą ir įvertinimą, ar dėl tokio pakeitimo reikia priimti papildomų IRT apsaugos priemonių.

2. Atlikę reikšmingus savo IRT sistemų pakeitimus, pagrindinės sandorio šalys ir centriniai vertybinių popierių depozitoriumai savo IRT sistemas visapusiškai testuoja imituodami nepalankiausias sąlygas.

Pagrindinės sandorių šalys į pirmoje pastraipoje nurodyto testavimo planavimą ir atlikimą, kai tinkama, įtraukia:

a) tarpuskaitos narius ir klientus;

b) sąveikias pagrindines sandorių šalis;

c) kitas suinteresuotąsias šalis.

Centriniai vertybinių popierių depozitoriumai į pirmoje pastraipoje nurodyto testavimo planavimą ir atlikimą, kai tinkama, įtraukia:

a) naudotojus;

b) ypatingos svarbos komunalinių paslaugų ir ypatingos svarbos paslaugų teikėjus;

c) kitus centrinius vertybinių popierių depozitoriumus;

d) kitas rinkos infrastruktūras;

e) visas kitas įstaigas, su kuriomis centrinių vertybinių popierių depozitoriumus, kaip nustatyta jų IRT veiklos tęstinumo politikoje, sieja tarpusavio priklausomybės ryšiai.

8 SKIRSNIS

18 straipsnis

Fizinis ir aplinkos saugumas

1. Finansų sektoriaus subjektai nustato, dokumentuoja ir įgyvendina fizinio ir aplinkos saugumo politiką ir įtraukia ją į apsaugos priemones, kuriomis siekiama išsaugoti duomenų prieinamumą, autentiškumą, vientisumą ir konfidencialumą. Finansų sektoriaus subjektai tą politiką rengia atsižvelgdami į kibernetinių grėsmių aplinką, IRT turto ir prieinamo informacinio turto klasifikaciją pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir bendrą rizikos profilį.

2. 1 dalyje nurodyta fizinio ir aplinkos saugumo politika apima visus šiuos elementus:

a) nuorodą į prieigos valdymo teisių kontrolės politikos skirsnį, nurodytą 21 straipsnio pirmos pastraipos g punkte;

b) finansų sektoriaus subjekto patalpų ir duomenų centrų, finansų sektoriaus subjekto įvardytų jautrių specialių zonų, kuriose laikomas IRT turtas ir informacinis turtas, apsaugos nuo išpuolių, avarijų ir grėsmių bei pavojų aplinkai priemones;

c) priemones IRT turtui apsaugoti tiek finansų sektoriaus subjekto patalpose, tiek už jų ribų, atsižvelgiant į IRT rizikos vertinimo, susijusio su atitinkamu IRT turtu, rezultatus;

d) priemones, kuriomis įgyvendinant tinkamą priežiūrą užtikrinamas IRT turto, informacinio turto ir finansų sektoriaus subjekto fizinės prieigos kontrolės įrenginių prieinamumas, autentiškumas, vientisumas ir konfidencialumas;

e) priemones duomenų prieinamumui, autentiškumui, vientisumui ir konfidencialumui išsaugoti, be kita ko:

   i) tuščio darbo stalo politiką;

   ii) tuščio ekrano politiką, taikomą informacijos tvarkymo įrangai.

Taikant b punktą, apsaugos nuo grėsmių ir pavojų aplinkai priemonės turėtų būti proporcingos patalpų, duomenų centrų bei jautrių specialių zonų svarbumui ir juose vykdomų operacijų ar esančių IRT sistemų ypatingai svarbai.

Taikant c punktą, 1 dalyje nurodyta fizinio ir aplinkos saugumo politika apima priemones, kuriomis užtikrinama tinkama nepriežiūrimo IRT turto apsauga.

II skyrius

ŽMOGIŠKŲJŲ IŠTEKLIŲ POLITIKA IR PRIEIGOS KONTROLĖ

19 straipsnis

Žmogiškųjų išteklių politika

Finansų sektoriaus subjektai į savo žmogiškųjų išteklių politiką ar kitas atitinkamas politikas įtraukia visus šiuos su IRT saugumu susijusius elementus:

a) visų specifinių su IRT saugumu susijusių pareigų nustatymą ir priskyrimą;

b) finansų sektoriaus subjekto ir IRT paslaugas teikiančių trečiųjų šalių darbuotojams, naudojantiems finansų sektoriaus subjekto IRT turtą ar turintiems prie jo prieigą, taikomus reikalavimus:

i) susipažinti su finansų sektoriaus subjekto IRT saugumo politika, procedūromis ir protokolais ir jų laikytis;

ii) žinoti finansų sektoriaus subjekto įdiegtus pranešimų teikimo kanalus, padedančius aptikti neįprastą elgesį, be kita ko, atitinkamais atvejais pranešimų teikimo kanalus, nustatytus pagal Europos Parlamento ir Tarybos direktyvą (ES) 2019/1937 ([11]);

iii) nutraukus darbo santykius su finansų sektoriaus subjektu grąžinti finansų sektoriaus subjektui visą jam priklausantį turėtą IRT turtą ir materialųjį informacinį turtą.

20 straipsnis

Tapatybės duomenų tvarkymas

1. Finansų sektoriaus subjektai parengia, dokumentuoja, įgyvendina ir į prieigos valdymo teisių kontrolę įtraukia tapatybės duomenų tvarkymo politiką ir procedūras, kuriomis užtikrinamas fizinių asmenų ir sistemų, turinčių prieigą prie finansų sektoriaus subjektų informacijos, unikalios tapatybės nustatymas ir autentiškumo patvirtinimas, leidžiantys priskirti naudotojo prieigos teises pagal 21 straipsnį.

2. 1 dalyje nurodyta tapatybės duomenų tvarkymo politika ir procedūros apima visus šiuos elementus:

a) (nedarant poveikio 21 straipsnio pirmos pastraipos c punkto taikymui) kiekvienam finansų sektoriaus subjekto arba IRT paslaugas teikiančių trečiųjų šalių darbuotojui, kuris turi prieigą prie finansų sektoriaus subjekto informacinio turto ir IRT turto, suteiktą unikalią tapatybę, atitinkančią unikalią naudotojo paskyrą;

b) tapatybės duomenų ir paskyrų tvarkymo per gyvavimo ciklą procesą, apimantį visų paskyrų kūrimą, keitimą, peržiūrą ir atnaujinimą, laikiną atjungimą ir panaikinimą.

Taikydami a punktą, finansų sektoriaus subjektai registruoja visas priskirtas tapatybes. Tie registracijos įrašai saugomi po finansų sektoriaus subjekto reorganizacijos ar pasibaigus sutartiniams santykiams, nedarant poveikio saugojimo reikalavimams, nustatytiems taikytinoje Sąjungos ir nacionalinėje teisėje.

Taikydami b punktą, finansų sektoriaus subjektai tais atvejais, kai įmanoma ir tinkama, diegia automatinius tapatybės duomenų tvarkymo per gyvavimo ciklą proceso sprendimus.

21 straipsnis

Prieigos kontrolė

Finansų sektoriaus subjektai parengia, dokumentuoja, įgyvendina ir į prieigos valdymo teisių kontrolę įtraukia politiką, apimančią visus šiuos elementus:

a) prieigos prie IRT turto, įskaitant nuotolinę ir neatidėliotiną prieigą, teisių priskyrimą remiantis būtinybės žinoti, būtinybės naudoti ir minimaliosios prieigos teisės principais;

b) pareigų atskyrimą, kuriuo užkertamas kelias neteisėtai prieigai prie ypatingos svarbos duomenų arba kelių prieigos teisių priskyrimui, galinčiam sudaryti sąlygas apeiti kontrolės priemones;

c) nuostatą dėl naudotojų atskaitingumo, kuria kuo labiau ribojamas beasmenių ir bendrųjų paskyrų naudojimas ir užtikrinama, kad visada būtų galima identifikuoti IRT sistemose veiksmus atlikusius naudotojus;

([11]) 2019 m. spalio 23 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos (OL L 305, 2019 11 26, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) nuostatą dėl prieigos prie IRT turto apribojimų, kuria nustatomos kontrolės ir kitos priemonės, kuriomis užkertamas kelias neteisėtai prieigai;

e) paskyrų administravimo procedūras, pagal kurias suteikiamos, keičiamos ar panaikinamos prieigos prie naudotojų ir beasmenių paskyrų, įskaitant beasmenes administratorių paskyras, teisės, įskaitant nuostatas dėl visų šių elementų:

   i) vaidmenų ir pareigų, susijusių su prieigos teisių suteikimu, peržiūra ir panaikinimu, priskyrimo;

   ii) privilegijuotos, neatidėliotinos ir administratoriaus prieigos prie visų IRT sistemų priskyrimo remiantis būtinybe naudoti arba *ad hoc* pagrindu;

   iii) neatidėliotino prieigos teisių panaikinimo nutraukus darbo santykius arba tais atvejais, kai prieiga nebebūtina;

   iv) prieigos teisių atnaujinimo, kai būtini pakeitimai ir bent kartą per metus visų IRT sistemų, išskyrus IRT sistemas, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, atveju ir bent kas šešis mėnesius IRT sistemų, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos, atveju;

f) autentiškumo patvirtinimo metodus, įskaitant:

   i) autentiškumo patvirtinimo metodų, kurie yra proporcingi klasifikacijai pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir bendram IRT turto rizikos profiliui ir kuriais atsižvelgiama į pažangiausią praktiką, taikymą;

   ii) saugesnio autentiškumo patvirtinimo metodų pagal pažangiausią praktiką ir metodus taikymą nuotolinei prieigai prie finansų sektoriaus subjekto tinklo, privilegijuotai prieigai, prieigai prie IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, ar viešai prieinamo IRT turto;

g) fizinės prieigos kontrolės priemones, įskaitant:

   i) fizinių asmenų, turinčių leidimą patekti į finansų sektoriaus subjekto įvardytas patalpas, duomenų centrus ir jautrias specialias zonas, kuriose yra laikomas IRT ir informacinis turtas, tapatybės nustatymą ir registravimą;

   ii) fizinės prieigos prie ypatingos svarbos IRT turto teisių suteikimą tik įgaliotiems asmenims remiantis būtinybės žinoti ir minimaliosios prieigos teisės principais, taip pat *ad hoc* pagrindu;

   iii) fizinės prieigos prie finansų sektoriaus subjekto įvardytų patalpų, duomenų centrų ir jautrių specialių zonų, kuriose yra laikomas IRT ir (arba) informacinis turtas, stebėseną;

   iv) fizinės prieigos teisių peržiūrą siekiant užtikrinti, kad nebūtinos prieigos teisės būtų nedelsiant panaikintos.

Taikydami e punkto i papunktį, finansų sektoriaus subjektai nustato saugojimo laikotarpį atsižvelgdami į veiklos ir informacijos saugumo tikslus, įvykio registravimo registracijos žurnaluose priežastis ir IRT rizikos vertinimo rezultatus.

Taikydami e punkto ii papunktį, kai įmanoma, finansų sektoriaus subjektai naudoja specialias paskyras administracinėms užduotims, susijusioms su IRT sistemomis, atlikti. Tais atvejais, kai įmanoma ir tinkama, finansų sektoriaus subjektai diegia automatinius privilegijuotos prieigos valdymo sprendimus.

Taikant g punkto i papunktį, tapatybės nustatymas ir registravimas turėtų būti proporcingi patalpų, duomenų centrų bei jautrių specialių zonų svarbumui ir juose vykdomų operacijų ar esančių IRT sistemų ypatingai svarbai.

Taikant g punkto iii papunktį, stebėsena turėtų būti proporcinga klasifikacijai pagal Reglamento (ES) 2022/2554 8 straipsnio 1 dalį ir zonos, į kurią patenkama, ypatingai svarbai.

III SKYRIUS

SU IRT SUSIJUSIŲ INCIDENTŲ APTIKIMAS IR REAGAVIMAS Į JUOS

22 straipsnis

Su IRT susijusių incidentų valdymo politika

Finansų sektoriaus subjektai parengia, dokumentuoja, įgyvendina ir į mechanizmus, kuriais aptinkama neįprasta veikla, be kita ko IRT tinklo veikimo problemos ir su IRT susiję incidentai, įtraukia su IRT susijusių incidentų valdymo politiką, kuria jie:

a) dokumentuoja su IRT susijusių incidentų valdymo procesą, nurodytą Reglamento (ES) 2022/2554 17 straipsnyje;

b) sudaro sąrašą svarbių kontaktų su vidaus funkcijas atliekančiais darbuotojais ir išorės suinteresuotaisiais subjektais, tiesiogiai dalyvaujančiais IRT operacijų saugumo veikloje, be kita ko, susijusioje su:

   i) kibernetinių grėsmių aptikimu ir stebėsena;

   ii) neįprastos veiklos aptikimu;

   iii) pažeidžiamumų valdymu;

c) nustato, įgyvendina ir valdo techninius, organizacinius ir operacinius mechanizmus, palaikančius su IRT susijusių incidentų valdymo procesą, įskaitant mechanizmus, leidžiančius nedelsiant aptikti neįprastą veiklą ir elgesį pagal šio reglamento 23 straipsnį;

d) saugo visus su IRT susijusiais incidentais susijusius įrodymus laikotarpį, kuris yra ne ilgesnis, nei reikia tais tikslais, kuriais renkami duomenys, ir proporcingas paveiktų veiklos funkcijų, palaikymo procesų ir IRT bei informacinio turto ypatingai svarbai, pagal Komisijos deleguotojo reglamento (ES) 2024/1772 ([12]) 15 straipsnį ir visus taikytinus saugojimo reikalavimus pagal Sąjungos teisę;

e) nustato ir įgyvendina mechanizmus, kuriais analizuojami reikšmingi ar pasikartojantys su IRT susiję incidentai ir su IRT susijusių incidentų skaičiaus ir vyksmo modeliai.

Taikydami d punktą, finansų sektoriaus subjektai saugo tame punkte nurodytus įrodymus saugiu būdu.

23 straipsnis

Neįprastos veiklos aptikimas ir su IRT susijusių incidentų aptikimo ir reagavimo į juos kriterijai

1. Finansų sektoriaus subjektai nustato aiškius vaidmenis ir pareigas, kad galėtų veiksmingai aptikti su IRT susijusius incidentus bei neįprastą veiklą ir reaguoti į juos.

2. Mechanizmas, skirtas neįprastai veiklai, įskaitant IRT tinklo veikimo problemas ir su IRT susijusius incidentus, skubiai aptikti, kaip nurodyta Reglamento (ES) 2022/2554 10 straipsnio 1 dalyje, sudaro sąlygas finansų sektoriaus subjektams:

a) rinkti, stebėti ir analizuoti:

   i) vidaus ir išorės veiksnius, įskaitant bent pagal šio reglamento 12 straipsnį pildytus registracijos žurnalus, informaciją iš veiklos ir IRT funkcijų ir visas finansų sektoriaus subjekto naudotojų praneštas problemas;

   ii) galimas vidaus ir išorės kibernetines grėsmes, atsižvelgiant į priešiškų subjektų dažniausiai naudojamus scenarijus ir žvalgybos informacija apie grėsmes grindžiamus scenarijus;

([12]) 2024 m. kovo 13 d. Komisijos deleguotasis reglamentas (ES) 2024/1772, kuriuo Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 papildomas techniniais reguliavimo standartais, kuriais patikslinami su IRT susijusių incidentų ir kibernetinių grėsmių klasifikavimo kriterijai, nustatomos reikšmingumo ribos ir nurodomi pranešimų apie didelius incidentus duomenys (OL L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) finansų sektoriaus subjektui IRT paslaugas teikiančios trečiosios šalies pranešimus apie su IRT susijusius incidentus, kurie aptikti IRT paslaugas teikiančios trečiosios šalies sistemose bei tinkluose ir gali daryti poveikį finansų sektoriaus subjektui;

b) identifikuoti neįprastą veiklą ir elgesį ir įgyvendinti priemones, įspėjančias apie neįprastą veiklą ir elgesį, susijusius bent su IRT turtu ir informaciniu turtu, kuriais palaikomos ypatingos svarbos arba svarbios funkcijos;

c) teikti pirmenybę b punkte nurodytiems įspėjimams, kad aptiktus su IRT susijusius incidentus būtų galima suvaldyti per numatytą sprendimo laiką, nurodytą finansų sektoriaus subjektų, tiek darbo, tiek ne darbo valandomis;

d) automatiškai ar rankiniu būdu registruoti, analizuoti ir įvertinti visą aktualią informaciją apie visą neįprastą veiklą ir elgesį.

Taikant b punktą, tame punkte nurodytos priemonės apima priemones, automatiškai siunčiančias įspėjimus pagal iš anksto nustatytas taisykles, skirtas anomalijoms, darančioms poveikį duomenų šaltinių ar registracijos žurnalų rinkinių išsamumui ir vientisumui, aptikti.

3. Finansų sektoriaus subjektai apsaugo visus neįprastos veiklos įrašus nuo neteisėto keitimo ir neteisėtos prieigos saugojimo, perdavimo ir atitinkamais atvejais naudojimo metu.

4. Finansų sektoriaus subjektai registruoja visą aktualią informaciją apie kiekvieną aptiktą neįprastą veiklą taip, kad būtų galima:

a) nustatyti datą ir laiką, kada įvyko neįprasta veikla;

b) nustatyti datą ir laiką, kada aptikta neįprasta veikla;

c) nustatyti neįprastos veiklos rūšį.

5. Finansų sektoriaus subjektai atsižvelgia į visus šiuos kriterijus, pagal kuriuos būtų galima inicijuoti su IRT susijusių incidentų aptikimo ir reagavimo į juos procesus, nurodytus Reglamento (ES) 2022/2554 10 straipsnio 2 dalyje:

a) požymius, kad IRT sistemoje ar tinkle galėjo būti vykdoma kenkėjiška veikla arba kad tokia IRT sistema ar tinklas galėjo būti užvaldyti;

b) aptiktą duomenų praradimą, susijusį su duomenų prieinamumu, autentiškumu, vientisumu ir konfidencialumu;

c) aptiktą neigiamą poveikį finansų sektoriaus subjekto sandoriams ir operacijoms;

d) IRT sistemų ir tinklo neprieinamumą.

6. Taikydami 5 dalį, finansų sektoriaus subjektai turėtų atsižvelgti į tai, ar paveiktos paslaugos yra ypatingos svarbos.

IV SKYRIUS

IRT VEIKLOS TĘSTINUMO VALDYMAS

24 straipsnis

IRT veiklos tęstinumo politikos komponentai

1. Finansų sektoriaus subjektai į Reglamento (ES) 2022/2554 11 straipsnio 1 dalyje nurodytą IRT veiklos tęstinumo politiką įtraukia visus šiuos elementus:

a) toliau nurodytų dalykų aprašymą:

i) IRT veiklos tęstinumo politikos tikslų, įskaitant IRT ir bendro veiklos tęstinumo tarpusavio ryšį, atsižvelgiant į Reglamento (ES) 2022/2554 11 straipsnio 5 dalyje nurodytos poveikio veiklai analizės rezultatus;

ii) IRT veiklos tęstinumo politikos priemonių, planų, procedūrų ir mechanizmų masto, įskaitant apribojimus ir išimtis;

iii) IRT veiklos tęstinumo politikos priemonių, planų, procedūrų ir mechanizmų taikymo termino;

iv) kriterijų, pagal kuriuos pradedami ir nustojami vykdyti IRT veiklos tęstinumo planai, IRT reagavimo ir veiklos atkūrimo planai ir krizių komunikacijos planai;

b) nuostatas dėl:

i) IRT veiklos tęstinumo politikos, įskaitant vaidmenis, pareigas ir incidentų sprendimo procedūras, įgyvendinimo valdymo ir organizavimo užtikrinant galimybę naudotis pakankamais ištekliais;

ii) IRT veiklos tęstinumo planų ir bendrų veiklos tęstinumo planų suderinimo, taikomo bent šiems elementams:

1) galimiems gedimo scenarijams, įskaitant šio reglamento 26 straipsnio 2 dalyje nurodytus scenarijus;

2) atkūrimo tikslams, nustatant, kad po sutrikimų finansų sektoriaus subjektas turi gebėti atkurti savo ypatingos svarbos arba svarbių funkcijų veikimą pagal veiklos atkūrimo laiko ir veiklos atkūrimo taško tikslus;

iii) įvykus dideliems veiklos sutrikimams taikomų IRT veiklos tęstinumo planų parengimo ir IRT veiklos tęstinumo veiksmų prioritetų nustatymo taikant rizika grindžiamą požiūrį;

iv) IRT reagavimo ir veiklos atkūrimo planų rengimo, testavimo ir peržiūros pagal šio reglamento 25 ir 26 straipsnius;

v) įgyvendinamų IRT veiklos tęstinumo politikos priemonių, planų, procedūrų ir mechanizmų veiksmingumo peržiūros pagal šio reglamento 26 straipsnį;

vi) IRT veiklos tęstinumo politikos suderinimo su:

1) komunikacijos politika, nurodyta Reglamento (ES) 2022/2554 14 straipsnio 2 dalyje;

2) komunikacijos ir krizių komunikacijos veiksmais, nurodytais Reglamento (ES) 2022/2554 11 straipsnio 2 dalies e punkte.

2. Be 1 dalyje nurodytų reikalavimų, pagrindinės sandorio šalys užtikrina, kad jų IRT veiklos tęstinumo politika:

a) būtų numatytas ilgiausias jų ypatingos svarbos funkcijų atkūrimo laikas, neviršijantis dviejų valandų;

b) būtų atsižvelgta į finansinių infrastruktūrų, įskaitant prekybos vietas, kurių tarpuskaitą atlieka pagrindinė sandorio šalis, vertybinių popierių atsiskaitymo sistemas, mokėjimo sistemas ir kredito įstaigas, kuriomis naudojasi pagrindinė sandorio šalis arba susieta pagrindinė sandorio šalis, išorės ryšius ir tarpusavio priklausomybę;

c) būtų reikalaujama nustatyti priemones, kuriomis:

i) pagal nelaimių scenarijus užtikrinamas pagrindinės sandorio šalies ypatingos svarbos arba svarbių funkcijų tęstinumas;

ii) palaikoma antrinė duomenų tvarkymo vieta, kuri gali užtikrinti pagrindinės sandorio šalies ypatingos svarbos arba svarbių funkcijų tęstinumą lygiai taip pat kaip pirminė vieta;

iii) palaikoma antrinė veiklos vieta ar nedelsiant suteikiama prieiga prie jos, kad darbuotojai galėtų užtikrinti paslaugos tęstinumą, jei pirminė veiklos vieta taptų neprieinama;

iv) įvertinamas poreikis turėti papildomų duomenų tvarkymo vietų, visų pirma tais atvejais, kai pirminės ir antrinės vietų rizikos profilio skirtumai nesuteikia pakankamai tikrumo, kad pagrindinės sandorio šalies veiklos tęstinumo tikslai bus įgyvendinti įvykus visiems scenarijams.

Taikydamos a punktą, pagrindinės sandorio šalys visais atvejais užbaigia dienos pabaigos procedūras ir mokėjimus reikiamą dieną ir laiku.

Taikant c punkto i papunktį, tame punkte nurodomomis priemonėmis sprendžiamos pakankamų žmogiškųjų išteklių, ilgiausio ypatingos svarbos funkcijų neveikimo laiko, veiklos perkėlimo į antrinę vietą ir atkūrimo toje vietoje problemos.

Taikant c punkto ii papunktį, tame papunktyje nurodytos antrinės duomenų tvarkymo vietos geografinės rizikos profilis turi skirtis nuo pirminės vietos geografinės rizikos profilio.

3. Be 1 dalyje nurodytų reikalavimų, centriniai vertybinių popierių depozitoriumai užtikrina, kad jų IRT veiklos tęstinumo politika:

a) būtų atsižvelgiama į naudotojų, ypatingos svarbos komunalinių paslaugų ir ypatingos svarbos paslaugų teikėjų, kitų centrinių vertybinių popierių depozitoriumų ir kitų rinkos infrastruktūrų ryšius ir tarpusavio priklausomybę;

b) būtų įpareigojama IRT veiklos tęstinumo priemonėmis užtikrinti, kad ypatingos svarbos arba svarbių funkcijų atkūrimo laiko tikslas neviršytų dviejų valandų.

4. Be 1 dalyje nurodytų reikalavimų, prekybos vietos užtikrina, kad jų IRT veiklos tęstinumo politika būtų užtikrinama, kad:

a) prekyba galėtų būti atnaujinta per dvi valandas arba nedaug ilgesnį nei dvi valandos laikotarpį po sutrikimą sukėlusio incidento;

b) didžiausias kiekis duomenų, kuriuos gali prarasti bet kuri prekybos vietos IT paslauga po sutrikimą sukėlusio incidento, būtų artimas nuliui.

25 straipsnis

IRT veiklos tęstinumo planų testavimas

1. Testuodami IRT veiklos tęstinumo planus pagal Reglamento (ES) 2022/2554 11 straipsnio 6 dalį, finansų sektoriaus subjektai atsižvelgia į savo atliktą poveikio veiklai analizę ir IRT rizikos vertinimą, nurodytą šio reglamento 3 straipsnio 1 dalies b punkte.

2. Testuodami 1 dalyje nurodytus savo IRT veiklos tęstinumo planus, finansų sektoriaus subjektai įvertina, ar yra pajėgūs užtikrinti savo ypatingos svarbos arba svarbių funkcijų tęstinumą. Tas testavimas:

a) atliekamas remiantis testavimo scenarijais, pagal kuriuos imituojami galimi sutrikimai, įskaitant tinkamą grupę blogiausių, bet tikėtinų scenarijų;

b) atitinkamais atvejais apima IRT paslaugų, kurias teikia IRT paslaugas teikiančios trečiosios šalys, testavimą;

c) finansų sektoriaus subjektų, išskyrus labai mažas įmones, kaip nurodyta Reglamento (ES) 2022/2554 11 straipsnio 6 dalies antroje pastraipoje, atveju, – apima pirminės IRT infrastruktūros pakeitimo atsarginiais pajėgumais, atsarginėmis kopijomis ir atsarginiais įrenginiais scenarijus;

d) turi tikslą patikrinti prielaidas, kuriomis grindžiami veiklos tęstinumo planai, įskaitant valdymo priemones ir krizių komunikacijos planus;

e) apima procedūras, skirtas patikrinti finansų sektoriaus subjekto darbuotojų, IRT paslaugas teikiančių trečiųjų šalių, IRT sistemų ir IRT paslaugų gebėjimą tinkamai reaguoti į scenarijus, į kuriuos deramai atsižvelgta pagal 26 straipsnio 2 dalį.

Taikydami a punktą, finansų sektoriaus subjektai visada į testavimą įtraukia scenarijus, svarstytus rengiant veiklos tęstinumo planus.

Taikydami b punktą, finansų sektoriaus subjektai deramai atsižvelgia į scenarijus, susijusius su IRT paslaugas teikiančių trečiųjų šalių nemokumu ar sutrikimais arba, kai aktualu, susijusius su politine rizika IRT paslaugas teikiančių trečiųjų šalių jurisdikcijose.

Taikydami c punktą, finansų sektoriaus subjektai patikrina, ar bent ypatingos svarbos arba svarbios funkcijos gali būti tinkamai vykdomos pakankamą laikotarpį ir ar gali būti atkurtas įprastas veikimas.

3. Be 2 dalyje nurodytų reikalavimų, pagrindinės sandorio šalys į 1 dalyje nurodytą IRT veiklos tęstinumo planų testavimą įtraukia:

a) tarpuskaitos narius;

b) išorės tiekėjus;

c) atitinkamas finansinės infrastruktūros įstaigas, su kuriomis pagrindines sandorio šalis, kaip nustatyta jų veiklos tęstinumo politikoje, sieja tarpusavio priklausomybės ryšiai.

4. Be 2 dalyje nurodytų reikalavimų, centriniai vertybinių popierių depozitoriumai į 1 dalyje nurodytą IRT veiklos tęstinumo planų testavimą atitinkamais atvejais įtraukia:

a) centrinių vertybinių popierių depozitoriumų naudotojus;

b) ypatingos svarbos komunalinių paslaugų ir ypatingos svarbos paslaugų teikėjus;

c) kitus centrinius vertybinių popierių depozitoriumus;

d) kitas rinkos infrastruktūras;

e) visas kitas įstaigas, su kuriomis centrinių vertybinių popierių depozitoriumus, kaip nustatyta jų veiklos tęstinumo politikoje, sieja tarpusavio priklausomybės ryšiai.

5. Finansų sektoriaus subjektai 1 dalyje nurodyto testavimo rezultatus dokumentuoja. Visi atliekant tą testavimą nustatyti trūkumai yra analizuojami, šalinami ir informacija apie juos pateikiama valdymo organui.

26 straipsnis

IRT reagavimo ir veiklos atkūrimo planai

1. Rengdami Reglamento (ES) 2022/2554 11 straipsnio 3 dalyje nurodytus IRT reagavimo ir veiklos atkūrimo planus, finansų sektoriaus subjektai atsižvelgia į savo atliktos poveikio veiklai analizės rezultatus. Tie IRT reagavimo ir veiklos atkūrimo planai:

a) nustato sąlygas, kuriomis šie planai pradedami ar baigiami vykdyti, ir visas tokio pradėjimo ar užbaigimo išimtis;

b) aprašo veiksmus, kurių reikia imtis siekiant užtikrinti bent IRT sistemų ir paslaugų, kuriomis palaikomos finansų sektoriaus subjekto ypatingos svarbos arba svarbios funkcijos, prieinamumą, vientisumą, tęstinumą ir atkūrimą;

c) siekia įvykdyti finansų sektoriaus subjekto operacijų atkūrimo tikslus;

d) yra dokumentuoti ir prieinami darbuotojams, dalyvaujantiems įgyvendinant IRT reagavimo ir veiklos atkūrimo planus, bei nedelsiant pasiekiami neatidėliotinu atveju;

e) numato tiek trumpalaikio, tiek ilgalaikio atkūrimo variantus, be kita ko, dalinį sistemų atkūrimą;

f) nustato IRT reagavimo ir veiklos atkūrimo planų tikslus ir sąlygas, kuriomis galima deklaruoti sėkmingą tų planų įvykdymą.

Taikydami d punktą, finansų sektoriaus subjektai aiškiai nustato vaidmenis ir pareigas.

2. 1 dalyje nurodytuose IRT reagavimo ir veiklos atkūrimo planuose nustatomi atitinkami scenarijai, įskaitant didelių veiklos sutrikimų scenarijus ir didesnės sutrikimų tikimybės scenarijus. Pagal tuos planus parengiami scenarijai, grindžiami esama informacija apie grėsmes ir patirtį, įgytą ankstesnių veiklos sutrikimų atvejais. Finansų sektoriaus subjektai deramai atsižvelgia į šiuos scenarijus:

a) kibernetinius išpuolius ir pirminės IRT infrastruktūros pakeitimą atsarginiais pajėgumais, atsarginėmis kopijomis ir atsarginiais įrenginiais;

b) scenarijus, pagal kuriuos ypatingos svarbos arba svarbios funkcijos vykdymo kokybė suprastėja iki nepriimtino lygio arba funkcija nebevykdoma ir kuriais tinkamai atsižvelgiama į galimą bet kurios atitinkamos IRT paslaugas teikiančios trečiosios šalies nemokumo ar kitokio įsipareigojimų nevykdymo poveikį;

c) dalinį arba visišką patalpų, įskaitant biurų ir veiklos patalpas bei duomenų centrus, sugadinimą;

d) reikšmingą IRT turto arba ryšių infrastruktūros sugadinimą;

e) kritinės dalies personalo ar darbuotojų, atsakingų už operacijų tęstinumo užtikrinimą, nebuvimą;

f) su klimato kaitos ir aplinkos būklės blogėjimo poveikiu susijusius įvykius, stichines nelaimes, pandemijas ir fizinius išpuolius, be kita ko, įsibrovimą ir teroristinius išpuolius;

g) vidaus subjektų išpuolius;

h) politinius ir socialinius neramumus, be kita ko, atitinkamais atvejais IRT paslaugas teikiančios trečiosios šalies jurisdikcijoje ir vietose, kuriose saugomi ir tvarkomi duomenys;

i) plataus masto elektros atjungimą.

3. Kai trumpuoju laikotarpiu neįmanoma taikyti pirminių atkūrimo priemonių dėl išlaidų, rizikos, logistikos ar nenumatytų aplinkybių, 1 dalyje nurodytuose IRT reagavimo ir veiklos atkūrimo planuose apsvarstomi alternatyvūs variantai.

4. Taikydami 1 dalyje nurodytus IRT reagavimo ir veiklos atkūrimo planus, finansų sektoriaus subjektai įvertina ir įgyvendina tęstinumo priemones, kuriomis mažinamas IRT paslaugas, kuriomis palaikomos finansų sektoriaus subjekto ypatingos svarbos arba svarbios funkcijos, teikiančių trečiųjų šalių trikčių poveikis.

V SKYRIUS

IRT RIZIKOS VALDYMO SISTEMOS PERŽIŪROS ATASKAITA

27 straipsnis

IRT rizikos valdymo sistemos peržiūros ataskaitos turinys ir forma

1. Finansų sektoriaus subjektai teikia IRT rizikos valdymo sistemos peržiūros ataskaitą, nurodytą Reglamento (ES) 2022/2554 6 straipsnio 5 dalyje, elektroniniu formatu, leidžiančiu naudoti paieškos funkciją.

2. Į 1 dalyje nurodytą ataskaitą finansų sektoriaus subjektai įtraukia šią informaciją:

a) įžanginį skirsnį, kuriame:

   i) aiškiai nustatomas finansų sektoriaus subjektas, kuris yra ataskaitos objektas, ir atitinkamais atvejais aprašoma jo grupės struktūra;

   ii) aprašomos ataskaitos rengimo aplinkybės: finansų sektoriaus subjekto paslaugų, veiklos ir operacijų pobūdis, mastas ir sudėtingumas, jo organizacinė struktūra, nustatytos ypatingos svarbos funkcijos, strategija, pagrindiniai tuo metu vykdomi projektai ar veikla, santykiai ir priklausomybė nuo savo darbuotojų teikiamų ar užsakytų IRT paslaugų ir sistemų arba tokių sistemų visiško praradimo arba smarkaus pablogėjimo pasekmės ypatingos svarbos arba svarbioms funkcijoms ir rinkos veiksmingumui;

   iii) apibendrinami svarbūs IRT rizikos valdymo sistemos pakeitimai nuo ankstesnės pateiktos ataskaitos;

   iv) pateikiama finansų sektoriaus subjekto dabartinio ir trumpo termino IRT rizikos profilio, grėsmių aplinkos, įvertinto jo kontrolės priemonių veiksmingumo ir saugumo būklės glausta santrauka;

b) datą, kurią finansų sektoriaus subjekto valdymo organas patvirtino ataskaitą;

c) IRT rizikos valdymo sistemos peržiūros priežasties aprašymą pagal Reglamento (ES) 2022/2554 6 straipsnio 5 dalį;

d) peržiūros laikotarpio pradžios ir pabaigos datas;

e) už peržiūrą atsakingą funkciją;

f) svarbių IRT rizikos valdymo sistemos pakeitimų ir patobulinimų nuo ankstesnės ataskaitos aprašymą;

g) peržiūros išvadų santrauką ir išsamią IRT rizikos valdymo sistemos silpnųjų vietų, trūkumų ir spragų, aptiktų per peržiūrą, kritiškumo analizę ir įvertinimą;

h) priemonių, kuriomis šalinamos nustatytos silpnosios vietos, trūkumai ir spragos, aprašymą, įskaitant visus šiuos elementus:

   i) priemonių, kurių imtasi nustatytoms silpnosioms vietoms, trūkumams ar spragoms ištaisyti, santrauką;

   ii) numatomą priemonių įgyvendinimo datą ir įgyvendinimo vidaus kontrolės datas, įskaitant informaciją apie tų priemonių įgyvendinimo eigą ataskaitos rengimo metu, atitinkamais atvejais paaiškinant, ar esama rizikos, kad terminų gali būti nesilaikoma;

   iii) naudotinas priemones ir už priemonių vykdymą atsakingas funkcijas, patikslinant, ar priemonės ir funkcijos yra vidaus, ar išorės;

   iv) numatytų priemonių pakeitimų poveikio finansų sektoriaus subjekto biudžeto, žmogiškiesiems ir materialiniams ištekliams, įskaitant visoms taisomosioms priemonėms įgyvendinti skirtus išteklius, aprašymą;

   v) informaciją apie kompetentingos institucijos informavimo atitinkamais atvejais procesą;

   vi) tais atvejais, kai nustatytoms silpnosioms vietoms, trūkumams ar spragoms taisomosios priemonės netaikomos, – išsamų kriterijų, taikomų analizuojant tų silpnųjų vietų, trūkumų ar spragų poveikį, vertinant ir pripažįstant susijusią liekamąją IRT riziką, paaiškinimą;

i) informaciją apie planuojamą tolesnę IRT rizikos valdymo sistemos plėtotę;

j) IRT rizikos valdymo sistemos peržiūros išvadas;

k) informaciją apie ankstesnes peržiūras, įskaitant:

   i) iki to momento atliktų ankstesnių peržiūrų sąrašą;

   ii) atitinkamais atvejais ankstesnėje ataskaitoje nustatytų taisomųjų priemonių įgyvendinimo būklę;

   iii) tais atvejais, kai paaiškėjo, kad ankstesnėje ataskaitoje nustatytos taisomosios priemonės yra neveiksmingos arba kelia nenumatytų problemų, – tų taisomųjų priemonių galimo patobulinimo arba tų nenumatytų problemų aprašymą;

l) rengiant ataskaitą naudotus informacijos šaltinius, įskaitant visus šiuos elementus:

   i) finansų sektoriaus subjektų, išskyrus labai mažas įmones, kaip nurodyta Reglamento (ES) 2022/2554 6 straipsnio 6 dalyje, atveju – vidaus auditų išvadas;

   ii) atitikties įvertinimo išvadas;

   iii) IRT priemonių, sistemų ir procesų skaitmeninės veiklos atsparumo testavimo rezultatus ir atitinkamais atvejais pažangaus testavimo, paremto grėsmėmis grindžiamu skverbimosi testavimu, rezultatus;

   iv) išorės šaltinius.

Taikant c punktą, tais atvejais, kai peržiūra pradėta laikantis priežiūros nurodymų arba vadovaujantis išvadomis, gautomis iš atitinkamo skaitmeninės veiklos atsparumo testavimo arba audito procesų, į ataskaitą įtraukiamos aiškios nuorodos į tokius nurodymus ar išvadas, leidžiančios nustatyti peržiūros pradėjimo priežastį. Tais atvejais, kai peržiūra pradėta po su IRT susijusių incidentų, į ataskaitą įtraukiamas visų su IRT susijusių incidentų sąrašas ir incidentų pirminių priežasčių analizė.

Taikant f punktą, į aprašymą įtraukiama pasikeitimų poveikio finansų sektoriaus subjekto skaitmeninės veiklos atsparumo strategijai, finansų sektoriaus subjekto IRT vidaus kontrolės sistemai ir finansų sektoriaus subjekto IRT rizikos valdymo sistemai analizė.

III ANTRAŠTINĖ DALIS

SUPAPRASTINTA IRT RIZIKOS VALDYMO SISTEMA, SKIRTA REGLAMENTO (ES) 2022/2554 16 STRAIPSNIO 1 DALYJE NURODYTIEMS FINANSŲ SEKTORIAUS SUBJEKTAMS

I SKYRIUS

SUPAPRASTINTA IRT RIZIKOS VALDYMO SISTEMA

28 straipsnis

Valdymas ir organizavimas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai įdiegia vidaus valdymo ir kontrolės sistemą, kuria užtikrinamas veiksmingas ir apdairus IRT rizikos valdymas, kad būtų užtikrintas aukšto lygio skaitmeninės veiklos atsparumas.

2. 1 dalyje nurodyti finansų sektoriaus subjektai, taikydami savo supaprastintą IRT rizikos valdymo sistemą, užtikrina, kad jų valdymo organas:

a) prisiimtų bendrą atsakomybę už tai, kad supaprastinta IRT rizikos valdymo sistema būtų sudarytos sąlygos įgyvendinti finansų sektoriaus subjekto veiklos strategiją pagal to finansų sektoriaus subjekto norimą prisiimti riziką, ir užtikrintų, kad tame kontekste būtų atsižvelgiama į IRT riziką;

b) nustatytų aiškias pareigas ir atsakomybę už visas su IRT susijusias užduotis;

c) nustatytų informacijos saugumo tikslus ir IRT reikalavimus;

d) tvirtintų, prižiūrėtų ir periodiškai peržiūrėtų:

   i) finansų sektoriaus subjekto informacinio turto klasifikaciją, nurodytą šio reglamento 30 straipsnio 1 dalyje, pagrindinės nustatytos rizikos sąrašą ir poveikio veiklai analizę bei susijusią politiką;

   ii) finansų sektoriaus subjekto veiklos tęstinumo planus ir reagavimo ir veiklos atkūrimo priemones, nurodytas Reglamento (ES) 2022/2554 16 straipsnio 1 dalies f punkte;

e) paskirstytų ir bent kartą per metus peržiūrėtų biudžetą, reikalingą tenkinti finansų sektoriaus subjekto skaitmeninės veiklos atsparumo poreikiams, susijusiems su visų rūšių ištekliais, įskaitant atitinkamas informuotumo apie IRT saugumą programas ir skaitmeninės veiklos atsparumo mokymą, taip pat visų darbuotojų IRT įgūdžius;

f) nustatytų ir įgyvendintų šios antraštinės dalies I, II ir III skyriuose nurodytą politiką ir priemones, skirtas finansų sektoriaus subjektui kylančiai IRT rizikai nustatyti, įvertinti ir valdyti;

g) nustatytų ir įgyvendintų procedūras, IRT protokolus ir priemones, kurių reikia visam informaciniam turtui ir IRT turtui apsaugoti;

h) užtikrintų, kad finansų sektoriaus subjekto darbuotojai turėtų pakankamai naujausių žinių ir įgūdžių IRT rizikai ir jos poveikiui finansų sektoriaus subjekto operacijoms suprasti ir įvertinti, atsižvelgiant į valdomą IRT riziką;

i) nustatytų atskaitomybės reikalavimus, įskaitant informacijos apie informacijos saugumą ir skaitmeninės veiklos atsparumą teikimo valdymo organui periodiškumą, formą ir turinį.

3. 1 dalyje nurodyti finansų sektoriaus subjektai gali, laikydamiesi Sąjungos ir nacionalinės sektorių teisės, perduoti IRT grupės vidaus subjektams arba IRT paslaugas teikiančioms trečiosioms šalims užduotis tikrinti atitiktį IRT rizikos valdymo reikalavimams. Tokio užduočių perdavimo atveju finansų sektoriaus subjektai išlieka visiškai atsakingi už atitikties IRT rizikos valdymo reikalavimams tikrinimą.

4. 1 dalyje nurodyti finansų sektoriaus subjektai užtikrina tinkamą kontrolės funkcijų ir vidaus audito funkcijų atskyrimą ir nepriklausomumą.

5. 1 dalyje nurodyti finansų sektoriaus subjektai užtikrina, kad auditoriai atliktų jų supaprastintos IRT rizikos valdymo sistemos vidaus auditą pagal finansų sektoriaus subjektų audito planą. Auditoriai turi turėti pakankamai žinių, įgūdžių ir ekspertinių žinių IRT rizikos srityje ir būti nepriklausomi. IRT auditų periodiškumas ir tikrinami aspektai turi atitikti finansų sektoriaus subjekto IRT riziką.

6. Priklausomai nuo 5 dalyje nurodyto audito rezultatų, 1 dalyje nurodyti finansų sektoriaus subjektai užtikrina svarbiausių IRT audito nustatytų trūkumų patikrinimą laiku ir ištaisymą.

29 straipsnis

Informacijos saugumo politika ir priemonės

1. Laikydamiesi supaprastintos IRT rizikos valdymo sistemos, Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina informacijos saugumo politiką. Ta informacijos saugumo politika nustatomi bendrieji principai ir taisyklės, būtini tų finansų sektoriaus subjektų duomenų ir teikiamų paslaugų konfidencialumui, vientisumui, prieinamumui ir autentiškumui apsaugoti.

2. Remdamiesi 1 dalyje nurodyta informacijos saugumo politika, 1 dalyje nurodyti finansų sektoriaus subjektai nustato ir įgyvendina IRT apsaugos priemones, kuriomis mažinamas jiems kylantis pavojus patirti IRT riziką, įskaitant rizikos mažinimo priemones, įgyvendinamas IRT paslaugas teikiančių trečiųjų šalių.

IRT apsaugos priemonės apima 30–38 straipsniuose nurodytas priemones.

30 straipsnis

Informacinio turto ir IRT turto klasifikavimas

1. Pagal Reglamento (ES) 2022/2554 16 straipsnio 1 dalies a punkte nurodytą supaprastintą IRT rizikos valdymo sistemą to straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai identifikuoja, suklasifikuoja ir dokumentuoja visas ypatingos svarbos arba svarbias funkcijas, jas palaikantį informacinį turtą ir IRT turtą ir jų tarpusavio priklausomybės ryšius. Prireikus finansų sektoriaus subjektai to identifikavimo rezultatus ir klasifikaciją peržiūri.

2. 1 dalyje nurodyti finansų sektoriaus subjektai identifikuoja visas IRT paslaugas teikiančių trečiųjų šalių palaikomas ypatingos svarbos arba svarbias funkcijas.

31 straipsnis

IRT rizikos valdymas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai į savo supaprastintą IRT rizikos valdymo sistemą įtraukia visus šiuos elementus:

a) priimtinos IRT rizikos lygio nustatymą, atsižvelgiant į finansų sektoriaus subjekto norimą prisiimti riziką;

b) IRT rizikos, kuri kyla finansų sektoriaus subjektui, nustatymą ir įvertinimą;

c) rizikos mažinimo strategijų, skirtų bent IRT rizikai, viršijančiai finansų sektoriaus subjekto priimtinos IRT rizikos lygį, nustatymą;

d) c punkte nurodytų rizikos mažinimo strategijų veiksmingumo stebėseną;

e) visos IRT ir informacijos saugumo rizikos, kylančios dėl bet kokio svarbaus IRT sistemų ar IRT paslaugų, procesų ar procedūrų pakeitimo ir dėl IRT saugumo testavimo rezultatų, taip pat po bet kokio didelio su IRT susijusio incidento, nustatymą ir įvertinimą.

2. 1 dalyje nurodyti finansų sektoriaus subjektai periodiškai atlieka ir dokumentuoja IRT rizikos vertinimą, proporcingą finansų sektoriaus subjekto IRT rizikos profiliui.

3. 1 dalyje nurodyti finansų sektoriaus subjektai nuolat stebi grėsmes ir pažeidžiamumus, svarbius jų ypatingos svarbos arba svarbioms funkcijoms, informaciniam turtui ir IRT turtui, ir periodiškai peržiūri rizikos scenarijus, darančius poveikį toms ypatingos svarbos arba svarbioms funkcijoms.

4. 1 dalyje nurodyti finansų sektoriaus subjektai nustato įspėjimo ribas ir kriterijus, pagal kuriuos būtų galima pradėti ir inicijuoti reagavimo į su IRT susijusius incidentus procesus.

32 straipsnis

Fizinis ir aplinkos saugumas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai nustato ir įgyvendina fizinio saugumo priemones, parengtas pagal grėsmių aplinką ir klasifikaciją pagal šio reglamento 30 straipsnio 1 dalį, bendrą IRT turto rizikos profilį ir prieinamą informacinį turtą.

2. 1 dalyje nurodytomis priemonėmis finansų sektoriaus subjektų patalpos ir atitinkamais atvejais jų duomenų centrai, kuriuose laikomas IRT turtas ir informacinis turtas, apsaugomi nuo neteisėtos prieigos, išpuolių, avarijų ir grėsmių bei pavojų aplinkai.

3. Apsauga nuo grėsmių ir pavojų aplinkai turėtų būti proporcinga atitinkamų patalpų ir atitinkamais atvejais duomenų centrų svarbumui ir juose vykdomų operacijų ar esančių IRT sistemų ypatingai svarbai.

II SKYRIUS

PAPILDOMI SISTEMŲ, PROTOKOLŲ IR PRIEMONIŲ IRT RIZIKAI MAŽINTI ELEMENTAI

33 straipsnis

Prieigos kontrolė

Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina loginės ir fizinės prieigos kontrolės procedūras, užtikrina jų vykdymą bei jas periodiškai peržiūri. Tos procedūros apima šiuos loginės ir fizinės prieigos kontrolės elementus:

a) prieigos prie finansų sektoriaus subjekto informacinio turto, IRT turto ir juo palaikomų funkcijų, taip pat prie ypatingos svarbos operacijų vietų teisės, įskaitant nuotolinę ir neatidėliotiną prieigą, yra administruojamos remiantis būtinybės žinoti, būtinybės naudoti ir minimaliosios prieigos teisės principais;

b) naudotojų atskaitingumą, kuriuo užtikrinama, kad būtų galima identifikuoti IRT sistemose veiksmus atlikusius naudotojus;

c) paskyrų administravimo procedūras, pagal kurias suteikiamos, keičiamos ar panaikinamos prieigos prie naudotojų ir beasmenių paskyrų, įskaitant beasmenes administratorių paskyras, teisės;

d) autentiškumo patvirtinimo metodus, kurie yra proporcingi klasifikacijai pagal 30 straipsnio 1 dalį bei bendram IRT turto rizikos profiliui ir pagrįsti pažangiausia praktika;

e) prieigos teisių periodišką peržiūrą ir panaikinimą, kai jos nebebūtinos.

Taikydamas c punktą, finansų sektoriaus subjektas priskiria privilegijuotą, neatidėliotiną ir administratoriaus prieigą prie visų IRT sistemų remdamasis būtinybe naudoti arba *ad hoc* pagrindu ir prieigą registruoja pagal 34 straipsnio pirmos pastraipos f punktą.

Taikydami d punktą, finansų sektoriaus subjektai taiko saugesnio autentiškumo patvirtinimo metodus, grindžiamus pažangiausia praktika, nuotolinei prieigai prie finansų sektoriaus subjekto tinklo, privilegijuotai prieigai ir prieigai prie viešai prieinamo IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos.

34 straipsnis

IRT operacijų saugumas

Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai, įgyvendindami savo sistemas, protokolus ir priemones, susijusius su visu IRT turtu:

a) stebi ir valdo viso IRT turto gyvavimo ciklą;

b) stebi, ar atitinkamais atvejais IRT turtą palaiko finansų sektoriaus subjektams IRT paslaugas teikiančios trečiosios šalys;

c) nustato savo IRT turto pajėgumo reikalavimus ir priemones, kuriomis išlaikomas ir gerinamas IRT sistemų prieinamumas bei veiksmingumas ir užkertamas kelias IRT pajėgumo trūkumams prieš jiems atsirandant;

d) atlieka automatinį IRT turto pažeidžiamumų skenavimą ir vertinimą, proporcingą klasifikacijai pagal šio reglamento 30 straipsnio 1 dalį ir bendram IRT turto rizikos profiliui, ir diegia pataisas, kuriomis šalinami identifikuoti pažeidžiamumai;

e) valdo riziką, susijusią su pasenusiu, nebepalaikomu ar senuoju IRT turtu;

f) registruoja įvykius, susijusius su loginės ir fizinės prieigos kontrole, IRT operacijomis, įskaitant sistemos ir tinklo srauto veiklą, ir IRT pakeitimų valdymu;

g) nustato ir įgyvendina priemones, kuriomis stebima ir analizuojama informacija apie neįprastą veiklą ir elgesį, susijusius su ypatingos svarbos arba svarbiomis IRT operacijomis;

h) įgyvendina priemones, kuriomis stebima aktuali ir naujausia informacija apie kibernetines grėsmes;

i) įgyvendina priemones, kuriomis nustatomas galimas informacijos nutekinimas, kenkėjiški kodai ir kitos grėsmės saugumui, taip pat viešai žinomi programinės ir aparatinės įrangos pažeidžiamumai, ir tikrinama, ar yra atitinkamų naujų saugumo naujinių.

Taikydami f punktą, finansų sektoriaus subjektai suderina registracijos žurnalų išsamumo lygį su jų paskirtimi ir IRT turto, pildančio tuos žurnalus, naudojimu.

35 straipsnis

Duomenų, sistemų ir tinklo saugumas

Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai parengia, įgyvendina ir į savo sistemas, protokolus ir priemones įtraukia apsaugos priemones, kuriomis užtikrinama tinklų apsauga nuo įsibrovimo bei netinkamo duomenų naudojimo ir išsaugomas duomenų prieinamumas, autentiškumas, vientisumas ir konfidencialumas. Visų pirma, atsižvelgdami į klasifikaciją pagal šio reglamento 30 straipsnio 1 dalį, finansų sektoriaus subjektai nustato šiuos elementus:

a) duomenų apsaugos jų saugojimo, perdavimo ir naudojimo metu priemonių identifikavimą ir įgyvendinimą;

b) apsaugos priemonių, susijusių su finansų sektoriaus subjekto duomenims persiųsti ir saugoti naudojama programine įranga, duomenų saugojimo laikmenomis, sistemomis ir galiniais įrenginiais, identifikavimą ir įgyvendinimą;

c) priemonių, kuriomis užkertamas kelias neteisėtam jungimuisi prie finansų sektoriaus subjekto tinklo ir apsaugomas tinklo duomenų srautas tarp finansų sektoriaus subjekto vidaus tinklų ir interneto bei kitų išorės jungčių, identifikavimą ir įgyvendinimą;

d) priemonių, kuriomis užtikrinamas duomenų prieinamumas, autentiškumas, vientisumas ir konfidencialumas perdavimo tinkle metu, identifikavimą ir įgyvendinimą;

e) patalpose laikomų ar išorėje saugomų duomenų, kurių finansų sektoriaus subjektui nebereikia rinkti ar saugoti, saugaus ištrynimo procesą;

f) patalpose laikomų ar išorėje saugomų duomenų saugojimo įrenginių, kuriuose įrašyta konfidenciali informacija, saugaus sunaikinimo procesą;

g) priemonių, kuriomis užtikrinama, kad nuotolinis darbas ir privačių galinių įrenginių naudojimas nedarytų neigiamo poveikio finansų sektoriaus subjekto gebėjimui vykdyti savo ypatingos svarbos veiklą tinkamai, saugiai ir laiku, identifikavimą ir įgyvendinimą.

36 straipsnis

IRT saugumo testavimas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai nustato ir įgyvendina IRT saugumo testavimo planą, pagal kurį patvirtinamas jų IRT apsaugos priemonių, parengtų pagal šio reglamento 33, 34, 35, 37 ir 38 straipsnius, veiksmingumas. Finansų sektoriaus subjektai užtikrina, kad tuo planu būtų atsižvelgiama į grėsmes ir pažeidžiamumus, identifikuotus taikant supaprastintą IRT rizikos valdymo sistemą, nurodytą šio reglamento 31 straipsnyje.

2. 1 dalyje nurodyti finansų sektoriaus subjektai peržiūri, įvertina ir testuoja IRT apsaugos priemones, atsižvelgdami į finansų sektoriaus subjekto IRT turto bendrą rizikos profilį.

3. 1 dalyje nurodyti finansų sektoriaus subjektai stebi ir vertina saugumo testų rezultatus ir nedelsdami atitinkamai atnaujina savo apsaugos priemones, jei tai susiję su IRT sistemomis, kuriomis palaikomos ypatingos svarbos arba svarbios funkcijos.

37 straipsnis

IRT sistemų įsigijimas, kūrimas ir priežiūra

Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai atitinkamais atvejais parengia ir įgyvendina IRT sistemų įsigijimo, kūrimo ir priežiūros procedūrą, taikydami rizika grindžiamą požiūrį. Ta procedūra:

a) užtikrinama, kad prieš įsigyjant ar kuriant IRT sistemas, atitinkamą veiklos funkciją vykdantis darbuotojas aiškiai nustatytų ir patvirtintų funkcinius ir nefunkcinius reikalavimus, įskaitant informacijos saugumo reikalavimus;

b) užtikrinamas IRT sistemų testavimas ir patvirtinimas prieš pirmą kartą jas naudojant ir prieš diegiant pakeitimus produkcinėje aplinkoje;

c) nustatomos priemonės, kuriomis mažinama netyčinio IRT sistemų pakeitimo ar tyčinio manipuliavimo jomis rizika jų kūrimo ir įgyvendinimo produkcinėje aplinkoje metu.

38 straipsnis

IRT projektų ir pakeitimų valdymas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT projektų valdymo procedūrą ir nustato su jos įgyvendinimu susijusius vaidmenis ir pareigas. Procedūra apima visus IRT projektų etapus nuo inicijavimo iki užbaigimo.

2. 1 dalyje nurodyti finansų sektoriaus subjektai parengia, dokumentuoja ir įgyvendina IRT pakeitimų valdymo procedūrą, kuria užtikrinama, kad visi IRT sistemų pakeitimai būtų registruojami, testuojami, vertinami, tvirtinami, įgyvendinami ir tikrinami kontroliuojamu būdu ir taikant tinkamas apsaugos priemones, kad būtų išsaugotas finansų sektoriaus subjekto skaitmeninės veiklos atsparumas.

III skyrius

IRT VEIKLOS TĘSTINUMO VALDYMAS

39 straipsnis

IRT veiklos tęstinumo plano komponentai

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai rengia savo IRT veiklos tęstinumo planus, atsižvelgdami į didelių veiklos sutrikimų rizikos ir jos galimo poveikio analizės rezultatus ir scenarijus, galimus jų IRT turtui, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, įskaitant kibernetinio išpuolio scenarijų.

2. 1 dalyje nurodyti IRT veiklos tęstinumo planai:

a) yra tvirtinami finansų sektoriaus subjekto valdymo organo;

b) yra dokumentuoti ir prieinami darbuotojams neatidėliotinu ar krizės atveju;

c) paskiriama pakankamai išteklių jiems įgyvendinti;

d) nustato planuojamą funkcijų atkūrimo lygį ir jų atkūrimo bei atnaujinimo terminus, taip pat pagrindinius vidaus ir išorės tarpusavio priklausomybės ryšius, įskaitant IRT paslaugas teikiančias trečiąsias šalis;

e) nustato sąlygas, kuriomis gali būti inicijuojamas IRT veiklos tęstinumo planų vykdymas, ir veiksmus, kurių reikia imtis siekiant užtikrinti finansų sektoriaus subjekto IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, prieinamumą, tęstinumą ir atkūrimą;

f) nustato ypatingos svarbos arba svarbių funkcijų, palaikymo procesų ir informacinio turto atkūrimo priemones, taip pat jų tarpusavio priklausomybės ryšius, kad būtų išvengta neigiamo poveikio finansų sektoriaus subjektų veikimui;

g) nustato atsarginių kopijų procedūras ir priemones, kuriose nurodoma duomenų, kurių atsarginės kopijos turi būti daromos, apimtis ir minimalus atsarginių kopijų darymo periodiškumas, remiantis tuos duomenis naudojančios funkcijos ypatinga svarba;

h) įvertina alternatyvius variantus, kai dėl išlaidų, rizikos, logistikos ar nenumatytų aplinkybių atkūrimas trumpuoju laikotarpiu gali būti neįmanomas;

i) nustato vidaus ir išorės komunikacijos tvarką, įskaitant incidentų sprendimo planus;

j) yra atnaujinami remiantis per incidentus įgyta patirtimi, testais, nauja rizika, identifikuotomis grėsmėmis, pasikeitusiais atkūrimo tikslais ir svarbiais finansų sektoriaus subjekto organizacinės struktūros ir IRT turto, kuriuo palaikomos ypatingos svarbos arba svarbios funkcijos, pakeitimais.

Taikant f punktą, tame punkte nurodytomis priemonėmis numatomas ypatingos svarbos paslaugas teikiančių trečiųjų šalių trikčių poveikio mažinimas.

40 straipsnis

Veiklos tęstinumo planų testavimas

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai testuoja šio reglamento 39 straipsnyje nurodytus savo veiklos tęstinumo planus, įskaitant tame straipsnyje nurodytus scenarijus, bent kartą per metus, kiek tai susiję su atsarginių kopijų ir atkūrimo procedūromis, arba po kiekvieno svarbaus veiklos tęstinumo plano pakeitimo.

2. Testuojant 1 dalyje nurodytus veiklos tęstinumo planus parodoma, kad toje dalyje nurodyti finansų sektoriaus subjektai gali išlaikyti savo veiklos gyvybingumą tol, kol bus atkurtos ypatingos svarbos operacijos, ir nustatyti visus tų planų trūkumus.

3. 1 dalyje nurodyti finansų sektoriaus subjektai veiklos tęstinumo planų testavimą dokumentuoja, o visus testuojant nustatytus trūkumus analizuoja, šalina ir praneša valdymo organui.

IV SKYRIUS

SUPAPRASTINTOS IRT RIZIKOS VALDYMO SISTEMOS PERŽIŪROS ATASKAITA

41 straipsnis

Supaprastintos IRT rizikos valdymo sistemos peržiūros ataskaitos turinys ir forma

1. Reglamento (ES) 2022/2554 16 straipsnio 1 dalyje nurodyti finansų sektoriaus subjektai teikia IRT rizikos valdymo sistemos peržiūros ataskaitą, nurodytą to straipsnio 2 dalyje, elektroniniu formatu, leidžiančiu naudoti paieškos funkciją.

2. 1 dalyje nurodytoje ataskaitoje pateikiama visa ši informacija:

a) įžanginis skirsnis, kuriame:

i) aprašomos ataskaitos rengimo aplinkybės: finansų sektoriaus subjekto paslaugų, veiklos ir operacijų pobūdis, mastas ir sudėtingumas, jo organizacinė struktūra, nustatytos ypatingos svarbos funkcijos, strategija, pagrindiniai tuo metu vykdomi projektai ar veikla, santykiai ir jo priklausomybė nuo savo darbuotojų teikiamų ar išorės teikiamų IRT paslaugų ir sistemų arba tokių sistemų visiško praradimo arba smarkaus pablogėjimo pasekmės ypatingos svarbos arba svarbioms funkcijoms ir rinkos veiksmingumui;

ii) pateikiama finansų sektoriaus subjekto nustatytos dabartinės ir trumpo termino IRT rizikos, grėsmių aplinkos, įvertinto jo kontrolės priemonių veiksmingumo ir saugumo būklės glausta santrauka;

iii) informacija apie sritį, kuri yra ataskaitos objektas;

iv) apibendrinami svarbūs IRT rizikos valdymo sistemos pakeitimai nuo ankstesnės ataskaitos;

v) apibendrinamas ir aprašomas svarbių supaprastintos IRT rizikos valdymo sistemos pakeitimų nuo ankstesnės ataskaitos poveikis;

b) atitinkamais atvejais nurodoma data, kurią finansų sektoriaus subjekto valdymo organas patvirtino ataskaitą;

c) peržiūros priežasčių aprašymas, įskaitant:

i) tais atvejais, kai peržiūra pradėta laikantis priežiūros nurodymų, – tokių nurodymų įrodymus;

ii) tais atvejais, kai peržiūra pradėta po su IRT susijusių incidentų, – visų tų su IRT susijusių incidentų sąrašą ir incidentų pirminių priežasčių analizę;

d) peržiūros laikotarpio pradžios ir pabaigos datos;

e) už ataskaitą atsakingas asmuo;

f) išvadų santrauka ir IRT rizikos valdymo sistemos silpnųjų vietų, trūkumų ir spragų peržiūros laikotarpiu kritiškumo įsivertinimas, įskaitant išsamią jų analizę;

g) nustatytos taisomosios priemonės supaprastintos IRT rizikos valdymo sistemos silpnosioms vietoms, trūkumams ir spragoms šalinti, taip pat numatoma tų priemonių įgyvendinimo data, įskaitant ankstesnėse ataskaitose nustatytų silpnųjų vietų, trūkumų ir spragų šalinimo pažangos, jei jie dar neištaisyti, stebėjimą;

h) supaprastintos IRT rizikos valdymo sistemos peržiūros bendros išvados, įskaitant visus tolesnius suplanuotus patobulinimus.

IV ANTRAŠTINĖ DALIS

BAIGIAMOSIOS NUOSTATOS

42 straipsnis

Įsigaliojimas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2024 m. kovo 13 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN