KOMISIJOS DELEGUOTASIS REGLAMENTAS (ES) 2022/1645

2022 m. liepos 14 d.

kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 nurodytoms organizacijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 748/2012 ir (ES) Nr. 139/2014

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2018 m. liepos 4 d. Europos Parlamento ir Tarybos reglamentą (ES) 2018/1139 dėl bendrųjų civilinės aviacijos taisyklių, ir kuriuo įsteigiama Europos Sąjungos aviacijos saugos agentūra, iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 2111/2005, (EB) Nr. 1008/2008, (ES) Nr. 996/2010, (ES) Nr. 376/2014 ir direktyvos 2014/30/ES ir 2014/53/ES bei panaikinami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 552/2004 ir (EB) Nr. 216/2008 bei Tarybos reglamentas (EEB) Nr. 3922/91 ([1]), ypač į jo 19 straipsnio 1 dalies g punktą ir 39 straipsnio 1 dalies b punktą,

kadangi:

(1) pagal Reglamento (ES) 2018/1139 II priedo 3.1 punkto b papunktyje nustatytus esminius reikalavimus, projektavimo ir gamybinės organizacijos turi įdiegti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

(2) be to, pagal Reglamento (ES) 2018/1139 VII priedo 2.2.1 ir 5.2 punktuose nustatytus esminius reikalavimus, aerodromų naudotojai ir už perono valdymo paslaugų teikimą atsakingos organizacijos turi įdiegti ir nuolat atnaujinti saugos rizikos valdymo sistemą;

(3) 1 ir 2 konstatuojamosiose dalyse nurodytos saugos rizikos šaltiniai gali būti įvairūs, pavyzdžiui, projektavimo ir techninės priežiūros trūkumai, su žmogaus galimybėmis susiję aspektai, su aplinka ir informacijos saugumu susijusios grėsmės. Todėl 1 ir 2 konstatuojamosiose dalyse nurodytų organizacijų įdiegtose valdymo sistemose turėtų būti atsižvelgiama ne tik į saugos riziką, kylančią dėl atsitiktinių įvykių, bet ir į saugos riziką, kylančią dėl grėsmių informacijos saugumui, kai esamais trūkumais gali pasinaudoti piktavališkų ketinimų turintys asmenys. Civilinės aviacijos aplinkoje ši informacijos saugumo rizika nuolat didėja, nes dabartinės informacinės sistemos tampa vis labiau tarpusavyje susijusios, be to, į jas vis dažniau taikosi piktavališki subjektai;

(4) su šiomis informacinėmis sistemomis susijusi rizika neapsiriboja galimais išpuoliais kibernetinėje erdvėje, bet apima ir grėsmes, kurios gali turėti įtakos procesams ir procedūroms, taip pat žmonių galimybėms;

(5) kad užtikrintų skaitmeninės informacijos ir duomenų saugumą, daug organizacijų jau taiko tarptautinius standartus (pavyzdžiui, ISO 27001). Šie standartai gali apimti ne visus civilinės aviacijos ypatumus;

(6) todėl tikslinga nustatyti informacijos saugumo rizikos, kuri gali turėti įtakos aviacijos saugai, valdymo reikalavimus;

(7) labai svarbu, kad tie reikalavimai apimtų įvairias aviacijos sritis ir jų sąsajas, nes aviacija yra itin glaudžiai sujungtų sistemų sąranga. Todėl jie turėtų būti taikomi visoms organizacijoms, kurios pagal galiojančius Sąjungos aviacijos saugos teisės aktus jau turi turėti valdymo sistemą;

(8) šiame reglamente nustatyti reikalavimai turėtų būti nuosekliai taikomi visose aviacijos srityse, kartu darant minimalų poveikį tose srityse jau taikomiems Sąjungos aviacijos saugos teisės aktams;

([1]) OL L 212, 2018 8 22, p. 1.

(9) šiame reglamente nustatytais reikalavimais neturėtų būti daromas poveikis informacijos saugumo ir kibernetinio saugumo reikalavimams, nustatytiems Komisijos įgyvendinimo reglamento (ES) 2015/1998 ([2]) priedo 1.7 punkte ir Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 ([3]) 14 straipsnyje;

(10) šiame teisės akte vartojamo termino „informacijos saugumas“ apibrėžtis neturėtų būti aiškinama kaip besiskirianti nuo Direktyvoje (ES) 2016/1148 pateiktos termino „tinklų ir informacinių sistemų saugumas“ apibrėžties;

(11) siekiant išvengti teisinių reikalavimų dubliavimosi, tais atvejais, kai į šio reglamento taikymo sritį įtrauktoms organizacijoms jau taikomi kitais 9 konstatuojamojoje dalyje nurodytais Sąjungos aktais nustatyti saugumo reikalavimai, kurių poveikis yra lygiavertis šio reglamento nuostatoms, atitiktis tiems saugumo reikalavimams turėtų būti laikoma atitiktimi šiame reglamente nustatytiems reikalavimams;

(12) į šio reglamento taikymo sritį įtrauktos organizacijos, kurioms jau taikomi Įgyvendinimo reglamente (ES) 2015/1998 nustatyti saugumo reikalavimai, taip pat turėtų laikytis šio reglamento I priedo (IS.D.OR.230 dalies „Informacijos saugumo išorės pranešimų sistema“) reikalavimų, nes į Įgyvendinimo reglamentą (ES) 2015/1998 neįtraukta nuostatų, susijusių su išorės pranešimų apie informacijos saugumo incidentus teikimu;

(13) Komisijos reglamentai (ES) Nr. 748/2012 ([4]) ir (ES) Nr. 139/2014 ([5]) turėtų būti iš dalies pakeisti siekiant susieti pirmiau nurodytuose reglamentuose nustatytas valdymo sistemas su šiame reglamente nustatytais informacijos saugumo valdymo reikalavimais;

(14) siekiant organizacijoms suteikti pakankamai laiko užtikrinti, kad būtų laikomasi šiuo reglamentu nustatytų naujų taisyklių ir procedūrų, šis reglamentas turėtų būti pradėtas taikyti praėjus 3 metams nuo jo įsigaliojimo dienos;

(15) šiame reglamente nustatyti reikalavimai grindžiami Nuomone Nr. 03/2021 ([6]), kurią Agentūra paskelbė pagal Reglamento (ES) 2018/1139 75 straipsnio 2 dalies b ir c punktus ir 76 straipsnio 1 dalį;

(16) laikydamasi Reglamento (ES) 2018/1139 128 straipsnio 4 dalies, Komisija konsultavosi su kiekvienos valstybės narės paskirtais ekspertais, vadovaudamasi 2016 m. balandžio 13 d. Tarpinstituciniame susitarime dėl geresnės teisėkūros ([7]) nustatytais principais,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Dalykas

Šiuo reglamentu nustatomi reikalavimai, kurių laikydamosi 2 straipsnyje nurodytos organizacijos, nustato ir valdo informacijos saugumo riziką, galinčią daryti poveikį aviacijos saugai ir turėti įtakos civilinės aviacijos tikslais naudojamoms informacinių ir ryšių technologijų sistemoms bei duomenims; aptinka informacijos saugumo įvykius ir nustato įvykius, laikomus informacijos saugumo incidentais, galinčiais turėti įtakos aviacijos saugai; reaguoja į tuos informacijos saugumo incidentus ir atkuria veiklą po tokių incidentų.

([2]) 2015 m. lapkričio 5 d. Komisijos įgyvendinimo reglamentas (ES) 2015/1998, kuriuo nustatomos išsamios bendrųjų pagrindinių aviacijos saugumo standartų įgyvendinimo priemonės (OL L 299, 2015 11 14, p. 1).

([3]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

([4]) 2012 m. rugpjūčio 3 d. Komisijos reglamentas (ES) Nr. 748/2012, kuriuo nustatomos orlaivio tinkamumo skraidyti sertifikavimo, orlaivio ir susijusių gaminių, dalių bei prietaisų aplinkosauginio sertifikavimo, taip pat projektavimo ir gamybinių organizacijų sertifikavimo įgyvendinimo taisyklės (OL L 224, 2012 8 21, p. 1).

([5]) 2014 m. vasario 12 d. Komisijos reglamentas (ES) Nr. 139/2014, kuriuo pagal Europos Parlamento ir Tarybos reglamentą (EB) Nr. 216/2008 nustatomi su aerodromais susiję reikalavimai ir administracinės procedūros (OL L 44, 2014 2 14, p. 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) OL L 123, 2016 5 12, p. 1.

2 straipsnis

Taikymo sritis

1. Šis reglamentas taikomas šioms organizacijoms:

a) gamybinėms organizacijoms ir projektavimo organizacijoms, kurioms taikomi Reglamento (ES) Nr. 748/2012 I priedo (21 dalies) A skirsnio G ir J poskyriai, išskyrus projektavimo ir gamybines organizacijas, kurios projektuoja ir (arba) gamina tik orlaivius ELA2, apibrėžtus Reglamento (ES) Nr. 748/2012 1 straipsnio 2 dalies j punkte;

b) aerodromų naudotojams ir perono valdymo paslaugų teikėjams, kuriems taikomas Reglamento (ES) Nr. 139/2014 III priedas „Organizacijoms taikomų reikalavimų dalis (ADR.OR dalis)“.

2. Šis reglamentas nedaro poveikio informacijos saugumo ir kibernetinio saugumo reikalavimams, nustatytiems Įgyvendinimo reglamento (ES) 2015/1998 priedo 1.7 punkte ir Direktyvos (ES) 2016/1148 14 straipsnyje.

3 straipsnis

Terminų apibrėžtys

Šiame reglamente vartojamų terminų apibrėžtys:

1) informacijos saugumas – tinklų ir informacinių sistemų konfidencialumo, vientisumo, autentiškumo ir prieinamumo išlaikymas;

2) informacijos saugumo įvykis – nustatytas sistemos, paslaugos ar tinklo būklės įvykis, rodantis galimą informacijos saugumo politikos pažeidimą arba informacijos saugumo kontrolės triktį, arba dar nežinoma situacija, kuri gali būti svarbi informacijos saugumui;

3) incidentas – neigiamą poveikį tinklų ir informacinių sistemų saugumui turintis įvykis, apibrėžtas Direktyvos (ES) 2016/1148 4 straipsnio 7 punkte;

4) informacijos saugumo rizika – dėl informacijos saugumo įvykio galimybės kylanti rizika organizacinėms civilinės aviacijos operacijoms, turtui, asmenims ir kitoms organizacijoms. Informacijos saugumo rizika yra susijusi su galimybe, kad, kilus grėsmei, bus pasinaudota informacinio turto arba informacinių išteklių grupės pažeidžiamumu;

5) grėsmė – galimas informacijos saugumo pažeidimas, atsirandantis esant subjektui, aplinkybėms, veiksmui arba įvykiui, galintiems padaryti žalos;

6) pažeidžiamumas – turto, sistemos, procedūrų, projektavimo, įgyvendinimo ar informacijos saugumo priemonių trūkumas arba silpnoji vieta, kuriais būtų galima pasinaudoti ir dėl kurių būtų pažeista informacijos saugumo politika.

4 straipsnis

Iš kitų Sąjungos teisės aktų kylantys reikalavimai

1. Jei 2 straipsnyje nurodyta organizacija atitinka Direktyvos (ES) 2016/1148 14 straipsnyje nustatytus saugumo reikalavimus, kurie yra lygiaverčiai šiame reglamente nustatytiems reikalavimams, atitiktis tiems saugumo reikalavimams laikoma atitiktimi šiame reglamente nustatytiems reikalavimams.

2. Jei 2 straipsnyje nurodyta organizacija yra operatorius arba subjektas, nurodytas valstybių narių nacionalinėse civilinės aviacijos saugumo programose, parengtose pagal Europos Parlamento ir Tarybos reglamento (EB) Nr. 300/2008 ([8]) 10 straipsnį, Įgyvendinimo reglamento (ES) 2015/1998 priedo 1.7 punkte nustatyti kibernetinio saugumo reikalavimai laikomi lygiaverčiais šiame reglamente nustatytiems reikalavimams, išskyrus šio reglamento priedo IS.D.OR.230 punktą, kurio turi būti laikomasi.

([8]) 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių ir panaikinantis Reglamentą (EB) Nr. 2320/2002 (OL L 97, 2008 4 9, p. 72).

3. Komisija, pasikonsultavusi su EASA ir Direktyvos (ES) 2016/1148 11 straipsnyje nurodyta Bendradarbiavimo grupe, gali paskelbti šiame reglamente ir Direktyvoje (ES) 2016/1148 nustatytų reikalavimų lygiavertiškumo vertinimo gaires.

5 straipsnis

Kompetentinga institucija

1. Už šio reglamento laikymosi patvirtinimą ir priežiūrą atsakinga institucija yra:

a) 2 straipsnio a punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 748/2012 I priedą (21 dalį);

b) 2 straipsnio b punkte nurodytų organizacijų – kompetentinga institucija, paskirta pagal Reglamento (ES) Nr. 139/2014 III priedą (ADR.OR dalį);

2. Šio reglamento tikslais valstybės narės gali paskirti nepriklausomą ir savarankišką subjektą, kuris atliktų 1 dalyje nurodytoms kompetentingoms institucijoms paskirtą funkciją ir pareigas. Tokiu atveju, siekiant užtikrinti veiksmingą visų reikalavimų, kuriuos turi atitikti organizacija, priežiūrą, nustatomos to subjekto ir 1 dalyje nurodytų kompetentingų institucijų veiklos koordinavimo priemonės.

6 straipsnis

Reglamento (ES) Nr. 748/2012 pakeitimas

Reglamento (ES) Nr. 748/2012 I priedas (21 dalis) iš dalies keičiamas taip:

1) turinys iš dalies keičiamas taip:

   a) po 21.A.139 antraštės įterpiama ši antraštė:

      „**21.A.139A Informacijos saugumo valdymo sistema**“;

   b) po 21.A.239 antraštės įterpiama ši antraštė:

      „**21.A.239A Informacijos saugumo valdymo sistema**“;

2) po 21.A.139 dalies įrašomas 21.A.139A punktas:

   „**21.A.139A Informacijos saugumo valdymo sistema**

   Be 21.A.139 punkte reikalaujamos gamybos valdymo sistemos, gamybinė organizacija pagal Komisijos deleguotąjį reglamentą (ES) 2022/1645 (*) parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.

   _____

   (*) 2022 m. liepos 14 d. Komisijos deleguotasis reglamentas (ES) 2022/1645, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 nurodytoms organizacijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 (OL L 248, 2022 9 26, p. 18).“;

3) po 21.A.239 punkto įrašomas 21.A.239A punktas:

   „**21.A.239A Informacijos saugumo valdymo sistema**

   Be projekto valdymo sistemos, kurios reikalaujama pagal 21.A.239 punktą, projektavimo organizacija pagal Deleguotąjį reglamentą (ES) 2022/1645 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“

7 straipsnis

Reglamento (ES) Nr. 139/2014 pakeitimas

Reglamento (ES) Nr. 139/2014 III priedas (ADR.OR dalis) iš dalies keičiamas taip:

1) po ADR.OR.D.005 punkto įrašomas ADR.OR.D.005A punktas:

„**ADR.OR.D.005A Informacijos saugumo valdymo sistema**

Aerodromo naudotojas pagal Komisijos deleguotąjį reglamentą (ES) 2022/1645 (*) parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.

_____

(*) 2022 m. liepos 14 d. Komisijos deleguotasis reglamentas (ES) 2022/1645, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 nurodytoms organizacijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 748/2012 ir (ES) Nr. 139/2014 (OL L 248, 2022 9 26, p. 18).“;

2) ADR.OR.D.007 punktas pakeičiamas taip:

„**ADR.OR.D.007 Oro navigacijos duomenų ir informacijos valdymas**

a) Įgyvendindamas valdymo sistemą, aerodromo naudotojas įdiegia ir nuolat atnaujina kokybės valdymo sistemą, apimančią šią veiklą:

1) jo oro navigacijos duomenų veiklą;

2) jo oro navigacijos informacijos teikimo veiklą.

b) Taikydamas valdymo sistemą, aerodromo naudotojas parengia saugumo valdymo sistemą gaunamų, rengiamų ar kitaip naudojamų operatyvinių duomenų saugumui užtikrinti, kad prieigą prie tų operatyvinių duomenų turėtų tik leidimą turintys asmenys.

c) Saugumo valdymo sistemoje turi būti nustatyti šie elementai:

1) procedūros, susijusios su duomenų saugumo rizikos vertinimu ir mažinimu, saugumo stebėjimu ir stiprinimu, saugumo peržiūromis ir patirties sklaida;

2) priemonės, kurias naudojant aptinkami saugumo pažeidimai ir atitinkamais saugumo signalais perspėjami darbuotojai;

3) saugumo pažeidimų poveikio suvaldymo ir taisomųjų veiksmų nustatymo priemonės bei rizikos mažinimo procedūros, kuriomis siekiama užkirsti kelią pažeidimų pasikartojimui.

d) Aerodromo naudotojas užtikrina savo darbuotojų patikimumo patikrinimą, susijusį su oro navigacijos duomenų saugumu.

e) Su informacijos saugumu susiję aspektai tvarkomi pagal ADR.OR.D.005A punktą.“;

3) po ADR.OR.F.045 punkto įrašomas ADR.OR.F.045A punktas:

„**ADR.OR.F.045A Informacijos saugumo valdymo sistema**

Už perono valdymo paslaugų teikimą atsakinga organizacija pagal Deleguotąjį reglamentą (ES) 2022/1645 parengia, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą, kad užtikrintų tinkamą informacijos saugumo rizikos, kuri gali daryti poveikį aviacijos saugumui, valdymą.“

8 straipsnis

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

Jis taikomas nuo 2025 m. spalio 16 d.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2022 m. liepos 14 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

PRIEDAS

INFORMACIJOS SAUGUMAS. ORGANIZACIJOMS TAIKOMI REIKALAVIMAI

[IS.D.OR DALIS]

IS.D.OR.100 Taikymo sritis

IS.D.OR.200 Informacijos saugumo valdymo sistema

IS.D.OR.205 Informacijos saugumo rizikos vertinimas

IS.D.OR.210 Informacijos saugumo rizikos priežiūra

IS.D.OR.215 Informacijos saugumo vidaus pranešimų teikimo sistema

IS.D.OR.220 Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

IS.D.OR.225 Reagavimas į pažeidimus, apie kuriuos pranešė kompetentingos institucijos

IS.D.OR.230 Informacijos saugumo išorės pranešimų teikimo sistema

IS.D.OR.235 Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

IS.D.OR.240 Reikalavimai darbuotojams

IS.D.OR.245 Įrašų saugojimas

IS.D.OR.250 Informacijos saugumo valdymo vadovas (ISVV)

IS.D.OR.255 Informacijos saugumo valdymo sistemos pakeitimai

IS.D.OR.260 Tęstinis tobulinimas

IS.D.OR.100 Taikymo sritis

Šioje dalyje nustatomi reikalavimai, kurių turi laikytis šio reglamento 2 straipsnyje nurodytos organizacijos.

IS.D.OR.200 Informacijos saugumo valdymo sistema (ISVS)

a) Siekdama 1 straipsnyje nustatytų tikslų, organizacija sukuria, įdiegia ir nuolat atnaujina informacijos saugumo valdymo sistemą (ISVS), kuria užtikrinama, kad organizacija:

   1) parengtų informacijos saugumo politiką, kurioje būtų nustatyti bendrieji organizacijos principai, susiję su galimu informacijos saugumo rizikos poveikiu aviacijos saugai;

   2) pagal IS.D.OR.205 punktą nustatytų ir peržiūrėtų informacijos saugumo riziką;

   3) pagal IS.D.OR.210 punktą parengtų ir įgyvendintų informacijos saugumo rizikos priežiūros priemones;

   4) pagal IS.D.OR.215 punktą įdiegtų informacijos saugumo vidaus pranešimų teikimo sistemą;

   5) pagal IS.D.OR.220 punktą parengtų ir įgyvendintų informacijos saugumo įvykiams aptikti skirtas priemones, nustatytų įvykius, kurie laikomi incidentais, galinčiais turėti įtakos aviacijos saugai, išskyrus leidžiamus atvejus pagal IS.D.OR.205 punkto e papunktį, imtųsi reagavimo į tuos informacijos saugumo incidentus priemonių ir atkurtų veiklą;

   6) įgyvendintų neatidėliotino reagavimo į informacijos saugumo incidentą arba pažeidžiamumą, darantį poveikį aviacijos saugai, priemones, apie kurias pranešė kompetentinga institucija;

   7) pagal IS.D.OR.225 punktą imtųsi tinkamų veiksmų, kad pašalintų pažeidimus, apie kuriuos pranešė kompetentinga institucija;

   8) pagal IS.D.OR.230 punktą įdiegtų išorės pranešimų teikimo sistemą, kad kompetentinga institucija galėtų imtis tinkamų veiksmų;

   9) su kitomis organizacijomis sudarydama sutartis dėl kurios nors IS.D.OR.200 punkte nurodytos veiklos dalies laikytųsi IS.D.OR.235 punkte nustatytų reikalavimų;

10) laikytųsi IS.D.OR.240 punkte nustatytų reikalavimų darbuotojams;

11) laikytųsi IS.D.OR.245 punkte nustatytų reikalavimų, susijusių su įrašų saugojimu;

12) stebėtų savo atitiktį šio reglamento reikalavimams ir teiktų grįžtamąją informaciją apie pažeidimus atsakingam vadovui arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovui, kad būtų užtikrintas veiksmingas taisomųjų veiksmų įgyvendinimas;

13) nedarydama poveikio taikytiniems pranešimo apie incidentus reikalavimams, saugotų bet kokios informacijos, kurią organizacija gavo iš kitų organizacijų, konfidencialumą, atsižvelgdama į jos slaptumo lygį.

b) Siekdama nuolat atitikti 1 straipsnyje nurodytus reikalavimus, organizacija pagal IS.D.OR.260 punktą įgyvendina nuolatinio tobulinimo procesą.

c) Organizacija pagal IS.D.OR.250 punktą dokumentais įformina visus pagrindinius procesus, procedūras, funkcijas ir atsakomybę, kurių reikia, kad būtų laikomasi IS.D.OR.200 punkto a papunkčio, ir nustato tų dokumentų keitimo tvarką. Tų procesų, procedūrų, funkcijų ir atsakomybės pakeitimai tvarkomi pagal IS.D.OR.255 punktą.

d) Procesai, procedūros, funkcijos ir atsakomybė, kuriuos organizacija nustatė siekdama laikytis IS.D.OR.200 punkto a papunkčio reikalavimų, turi atitikti jos veiklos pobūdį ir sudėtingumą, atsižvelgiant į tai veiklai būdingos informacijos saugumo rizikos vertinimą, ir gali būti integruoti į kitas esamas organizacijos jau įdiegtas valdymo sistemas.

e) Nedarydama poveikio pareigai laikytis pranešimų teikimo reikalavimų, nustatytų Europos Parlamento ir Tarybos reglamente (ES) Nr. 376/2014 ([1]), ir IS.D.OR.200 punkto a papunkčio 13 dalyje nustatytų reikalavimų, kompetentinga institucija organizacijai gali suteikti patvirtinimą nevykdyti a–d punktuose nurodytų reikalavimų ir susijusių reikalavimų, nustatytų IS.D.OR.205–IS.D.OR.260 punktuose, jei ji tai institucijai priimtinu būdu įrodo, kad jos veikla, infrastruktūra ir ištekliai, taip pat jos valdomos, teikiamos, gaunamos ir prižiūrimos paslaugos nekelia jokios informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, nei jai pačiai, nei kitoms organizacijoms. Patvirtinimas turi būti grindžiamas dokumentais pagrįstu informacijos saugumo rizikos vertinimu, kurį organizacija arba trečioji šalis atliko pagal IS.D.OR.205 punktą, o jį peržiūrėjo ir patvirtino jos kompetentinga institucija.

Tęstinį to patvirtinimo galiojimą kompetentinga institucija peržiūrės užbaigusi taikytiną priežiūros audito ciklą ir kas kartą, kai bus atliekami organizacijos darbo apimties pakeitimai.

IS.D.OR.205 Informacijos saugumo rizikos vertinimas

a) Organizacija nustato visus savo elementus, kuriems gali kelti grėsmę informacijos saugumo rizika. Tie elementai apima:

1) organizacijos veiklą, įrenginius ir išteklius, taip pat paslaugas, kurias organizacija valdo, teikia, gauna ar prižiūri;

2) įrangą, sistemas, duomenis ir informaciją, kurie padeda užtikrinti 1 punkte išvardytų elementų veikimą.

b) Organizacija nustato su kitomis organizacijomis turimas sąsajas, dėl kurių jai ir toms organizacijoms gali kelti grėsmę informacijos saugumo rizika.

c) Kiek tai susiję su a ir b punktuose nurodytais elementais ir sąsajomis, organizacija nustato informacijos saugumo riziką, kuri gali turėti įtakos aviacijos saugai. Dėl kiekvienos nustatytos rizikos organizacija:

1) nustato rizikos lygį pagal organizacijos nustatytą iš anksto parengtą klasifikaciją;

([1]) 2014 m. balandžio 3 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 376/2014 dėl pranešimo apie civilinės aviacijos įvykius, jų analizės ir tolesnės veiklos, kuriuo iš dalies keičiamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 996/2010 ir panaikinama Europos Parlamento ir Tarybos direktyva 2003/42/EB ir Komisijos reglamentai (EB) Nr. 1321/2007 ir (EB) Nr. 1330/2007 (OL L 122, 2014 4 24, p. 18).

2) kiekvieną riziką ir jos lygį susieja su atitinkamu elementu arba sąsaja, nustatytais pagal a ir b punktus.

1 punkte nurodytoje iš anksto parengtoje klasifikacijoje atsižvelgiama į galimą grėsmės scenarijaus atsiradimą ir jo pasekmių saugai sunkumą. Remdamasi ta klasifikacija ir atsižvelgdama į tai, ar yra įsidiegusi struktūrizuotą ir kartotinį veiklos rizikos valdymo procesą, organizacija turi gebėti nustatyti, ar rizika yra priimtina, arba tai, ar reikia taikyti rizikos priežiūrą pagal IS.D.OR.210 punktą.

Siekiant palengvinti abipusį rizikos vertinimų palyginamumą, nustatant rizikos lygį pagal 1 punktą atsižvelgiama į atitinkamą informaciją, gautą koordinuojant veiksmus su b punkte nurodytomis organizacijomis.

d) Organizacija peržiūri ir atnaujina pagal a, b ir c punktus atliktą rizikos vertinimą bet kuriuo iš šių atvejų:

1) pasikeitus elementams, kuriems gali kelti grėsmę informacijos saugumo rizika;

2) pasikeitus organizacijos ir kitų organizacijų sąsajoms arba rizikai, apie kurią pranešė kitos organizacijos;

3) pasikeitus informacijai ar žinioms, naudojamoms rizikai nustatyti, analizuoti ir klasifikuoti;

4) įgijus patirties vykdant informacijos saugumo incidentų analizę.

IS.D.OR.210 Informacijos saugumo rizikos priežiūra

a) Organizacija parengia pagal IS.D.OR.205 punktą nustatytos nepriimtinos rizikos mažinimo priemones, jas laiku įgyvendina ir nuolatos tikrina jų veiksmingumą. Tos priemonės organizacijai turi suteikti galimybę:

1) kontroliuoti aplinkybes, kurios prisideda prie faktinio grėsmės scenarijaus atsiradimo;

2) sumažinti su grėsmės scenarijaus išsipildymu susijusias pasekmes aviacijos saugai;

3) išvengti rizikos.

Tos priemonės neturi kelti jokios naujos galimos nepriimtinos rizikos aviacijos saugai.

b) IS.D.OR.240 punkto a ir b papunkčiuose nurodytas asmuo ir kiti susiję organizacijos darbuotojai informuojami apie rizikos vertinimo, atlikto pagal IS.D.OR.205 punktą, rezultatus, atitinkamus grėsmės scenarijus ir priemones, kurios turi būti įgyvendintos.

Organizacija taip pat informuoja organizacijas, su kuriomis ji turi sąsają pagal IS.D.OR.205 punkto b papunktį, apie joms bendrą riziką.

IS.D.OR.215 Informacijos saugumo vidaus pranešimų teikimo sistema

a) Organizacija sukuria vidaus pranešimų teikimo sistemą, kad būtų galima rinkti informaciją apie informacijos saugumo įvykius ir vertinti tuos įvykius, įskaitant įvykius, apie kuriuos turi būti pranešama pagal IS.D.OR.230 punktą.

b) Ta sistema ir IS.D.OR.220 punkte nurodytas procesas turi suteikti organizacijai galimybę:

1) nustatyti, kurie iš įvykių, apie kuriuos pranešta pagal a punktą, laikomi informacijos saugumo incidentais arba pažeidžiamumu, galinčiais turėti įtakos aviacijos saugai;

2) identifikuoti pagal 1 punktą nustatytų informacijos saugumo incidentų ir pažeidžiamumo priežastis ir juos lemiančius veiksnius, taip pat juos pašalinti taikant informacijos saugumo rizikos valdymo procesą pagal IS.D.OR.205 ir IS.D.OR.220 punktus;

3) užtikrinti, kad visa žinoma svarbi informacija, susijusi su informacijos saugumo incidentais ir pažeidžiamumu, nustatytais pagal 1 punktą, būtų įvertinta;

4) užtikrinti, kad prireikus būtų taikomas informacijos vidaus platinimo metodas.

c) Bet kuri organizacija, su kuria sudaroma sutartis ir dėl kurios organizacijai gali kilti informacijos saugumo rizika, galinti turėti įtakos aviacijos saugai, privalo pranešti organizacijai apie informacijos saugumo įvykius. Tie pranešimai teikiami taikant konkrečiuose sutartimi įformintuose susitarimuose nustatytas procedūras ir vertinami pagal b punktą.

d) Tyrimų srityje organizacija bendradarbiauja su kiekviena kita organizacija, kurios indėlis į jos veiklos informacijos saugumą yra reikšmingas.

e) Organizacija gali sujungti tą pranešimų teikimo sistemą su kitomis jau įsidiegtomis pranešimų teikimo sistemomis.

IS.D.OR.220 Informacijos saugumo incidentai. Aptikimas, reagavimas ir veiklos atkūrimas

a) Remdamasi pagal IS.D.OR.205 punktą atlikto rizikos vertinimo rezultatais ir pagal IS.D.OR.210 punktą atliktos rizikos priežiūros rezultatais, organizacija įgyvendina incidentų ir pažeidžiamumo, kurie rodo galimą nepriimtinos rizikos pasireiškimą ir kurie gali turėti įtakos aviacijos saugai, aptikimo priemones. Tomis aptikimo priemonėmis organizacijai suteikiama galimybė:

1) nustatyti nuokrypius nuo iš anksto nustatytų funkcinio veiksmingumo bazinių verčių;

2) aktyvuoti įspėjimus, kad bet kokio nuokrypio atveju būtų taikomos tinkamos reagavimo priemonės.

b) Organizacija įgyvendina priemones, kurios padeda reaguoti į bet kokias pagal a punktą nustatytas įvykio aplinkybes, kurios gali nulemti arba nulėmė informacijos saugumo incidentą. Tos reagavimo priemonės organizacijai turi suteikti galimybę:

1) inicijuoti reakciją į a punkto 2 papunktyje nurodytus įspėjimus, aktyvuojant iš anksto nustatytus išteklius ir veiksmų seką;

2) sustabdyti išpuolio plitimą ir išvengti visiško grėsmės scenarijaus išsipildymo;

3) kontroliuoti IS.D.OR.205 punkto a papunktyje apibrėžtų paveiktų elementų veikimą trikties režimu.

c) Organizacija įgyvendina priemones, kuriomis siekiama atkurti veiklą po informacijos saugumo incidentų, įskaitant, jei reikia, neatidėliotinas priemones. Tos veiklos atkūrimo priemonės organizacijai turi suteikti galimybę:

1) pašalinti incidentą sukėlusią aplinkybę arba apriboti ją iki toleruotino lygio;

2) per organizacijos iš anksto nustatytą veiklos atkūrimo laiką užtikrinti, kad paveiktų elementų, kurie apibrėžti IS.D.OR.205 punkto a papunktyje, būklė būtų saugi.

IS.D.OR.225 Reagavimas į pažeidimus, apie kuriuos pranešė kompetentingos institucijos

a) Gavusi kompetentingos institucijos pranešimą apie pažeidimus, organizacija:

1) nustato pagrindinę neatitikties priežastį (-is) bei tos neatitikties veiksnius;

2) parengia taisomųjų veiksmų planą;

3) kompetentingai institucijai priimtinu būdu įrodo, kad neatitiktis yra pašalinta.

b) A punkte nurodyti veiksmai atliekami per laikotarpį, dėl kurio susitarta su kompetentinga institucija.

IS.D.OR.230 Informacijos saugumo išorės pranešimų teikimo sistema

a) Organizacija įdiegia informacijos saugumo pranešimų sistemą, atitinkančią Reglamente (ES) Nr. 376/2014 ir jo deleguotuosiuose bei įgyvendinimo aktuose, jei tas reglamentas taikomas organizacijai, nustatytus reikalavimus.

b) Nedarant poveikio Reglamente (ES) Nr. 376/2014 nustatytoms pareigoms, organizacija užtikrina, kad apie bet kokį informacijos saugumo incidentą ar pažeidžiamumą, kurie gali kelti didelę riziką aviacijos saugai, būtų pranešama jos kompetentingai institucijai. Be to:

1) jei toks incidentas ar pažeidžiamumas daro poveikį orlaiviui arba susijusiai sistemai ar komponentui, organizacija apie tai taip pat praneša projekto patvirtinimo turėtojui;

2) jei toks incidentas ar pažeidžiamumas daro poveikį organizacijos naudojamai sistemai ar sudedamajai daliai, organizacija apie tai praneša organizacijai, atsakingai už sistemos ar sudedamosios dalies projektavimą.

c) Apie b punkte nurodytas aplinkybes organizacija praneša taip:

1) pranešimas pateikiamas kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba organizacijai, atsakingai už sistemos ar sudedamosios dalies projektavimą, kai tik organizacija sužino apie aplinkybę;

2) pranešimas pateikiamas kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba už sistemos ar sudedamosios dalies projektavimą atsakingai organizacijai kuo greičiau ir ne vėliau kaip per 72 valandas nuo momento, kai organizacija sužinojo apie aplinkybę, nebent tai būtų neįmanoma dėl išskirtinių sąlygų.

Pranešimas parengiamas kompetentingos institucijos nustatyta forma ir jame pateikiama visa svarbi informacija apie organizacijai žinomą aplinkybę;

3) kompetentingai institucijai ir, jei taikoma, projekto patvirtinimo turėtojui arba už sistemos ar sudedamosios dalies projektavimą atsakingai organizacijai pateikiama tolesnių veiksmų ataskaita, kurioje pateikiama išsami informacija apie veiksmus, kurių organizacija ėmėsi arba ketina imtis, kad atkurtų veiklą po incidento, ir apie veiksmus, kurių ji ketina imtis, kad ateityje užkirstų kelią panašiems informacijos saugumo incidentams.

Tolesnių veiksmų ataskaita pateikiama iš karto, kai tik nustatomi tie veiksmai, ir parengiama kompetentingos institucijos nustatyta forma.

IS.D.OR.235 Sutarčių dėl informacijos saugumo valdymo veiklos sudarymas

a) Organizacija užtikrina, kad tais atvejais, kai su kitomis organizacijomis sudaromos sutartys dėl bet kurios IS.D.OR.200 punkte nurodytos veiklos dalies, veikla, dėl kurios sudaryta sutartis, atitiktų šio reglamento reikalavimus, o organizacija, su kuria sudaryta sutartis, veiktų jos prižiūrima. Organizacija užtikrina, kad rizika, susijusi su veikla, dėl kurios sudaryta sutartis, būtų tinkamai valdoma.

b) Organizacija užtikrina, kad pateikusi prašymą kompetentinga institucija galėtų kreiptis į organizaciją, su kuria sudaryta sutartis, kad nustatytų, ar tebesilaikoma šiame reglamente nustatytų taikytinų reikalavimų.

IS.D.OR.240 Reikalavimai darbuotojams

a) Šio reglamento 2 straipsnio 1 dalies a ir b punktuose nurodytos organizacijos atsakingas vadovas arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovas, paskirtas pagal Reglamentą (ES) Nr. 748/2012 ir Reglamentą (ES) Nr. 139/2014, turi turėti tarnybinius įgaliojimus užtikrinti, kad visa pagal šį reglamentą reikalaujama veikla galėtų būti finansuojama ir vykdoma. Tas asmuo:

1) užtikrina, kad būtų prieinami visi šio reglamento reikalavimams įvykdyti būtini ištekliai;

2) parengia S.D.OR.200 punkto a papunkčio 1 dalyje nurodytą informacijos saugumo politiką ir skatina ją taikyti;

3) įrodo, kad bendrai išmano šį reglamentą.

b) Atsakingas vadovas arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovas paskiria asmenį arba asmenų grupę, kurie užtikrintų, kad organizacija laikytųsi šio reglamento reikalavimų, ir nustato jų įgaliojimų apimtį. Tas asmuo ar asmenų grupė tiesiogiai atsiskaito atsakingam vadovui arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovui ir turi turėti atitinkamų žinių, kvalifikaciją ir patirties, kad galėtų vykdyti savo pareigas. Procedūrose nustatoma, kas pavaduoja tam tikrą asmenį, jeigu jo ilgą laiką nebūtų.

c) Atsakingas vadovas arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovas paskiria asmenį arba asmenų grupę, kuriems pavedama administruoti IS.D.OR.200 punkto a papunkčio 12 dalyje nurodytą atitikties stebėsenos funkciją.

d) Jeigu organizacijos informacijos saugumo organizacinės struktūros, politika, procesai ir procedūros bendrai naudojami su kitomis organizacijomis arba pačios organizacijos dalyse, kurios nėra įtrauktos į patvirtinimą ar deklaraciją, atsakingas vadovas arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovas gali pavesti savo veiklą bendram atsakingam asmeniui.

Tokiu atveju, siekiant užtikrinti tinkamą informacijos saugumo valdymo integravimą organizacijoje, tarp atsakingo organizacijos vadovo arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovo ir bendro atsakingo asmens nustatomos veiksmų koordinavimo priemonės.

e) Atsakingas vadovas arba projektavimo organizacijos vadovas ar d punkte nurodytas bendras atsakingas asmuo turi turėti tarnybinius įgaliojimus kurti ir nuolat atnaujinti IS.D.OR.200 punktui įgyvendinti būtinas organizacines struktūras, politiką, procesus ir procedūras.

f) Organizacija įdiegia procesą, kuriuo užtikrinamas pakankamas skaičius darbuotojų, galinčių vykdyti šiame priede nurodytą veiklą.

g) Organizacija įdiegia procesą, kuriuo užtikrinama, kad f punkte nurodyti darbuotojai turėtų reikiamą kompetenciją savo užduotims atlikti.

h) Organizacija įdiegia procesą, kuriuo užtikrinama, kad darbuotojai būtų informuoti apie atsakomybę, susijusią su jiems pavestomis funkcijomis ir užduotimis.

i) Organizacija užtikrina, kad būtų tinkamai nustatyta darbuotojų, turinčių prieigą prie informacinių sistemų ir duomenų, kuriems taikomi šio reglamento reikalavimai, tapatybė ir patikimumas.

IS.D.OR.245 Įrašų saugojimas

a) Organizacija registruoja savo informacijos saugumo valdymo veiklą

1) Organizacija užtikrina, kad būtų archyvuojami ir atsekami šie įrašai:

i) visi gauti patvirtinimai ir visi susiję informacijos saugumo rizikos vertinimai pagal IS.D.OR.200 punkto e papunktį;

ii) sutartys dėl veiklos, nurodytos IS.D.OR.200 punkto a papunkčio 9 dalyje;

iii) įrašai apie IS.D.OR.200 punkto d papunktyje nurodytus pagrindinius procesus;

iv) įrašai apie IS.D.OR.205 punkte nurodytame rizikos vertinime nustatytą riziką ir IS.D.OR.210 punkte nurodytas susijusias rizikos priežiūros priemones;

v) įrašai apie informacijos saugumo incidentus ir pažeidžiamumą, apie kuriuos pranešta pagal IS.D.OR.215 ir IS.D.OR.230 punktuose nurodytas pranešimo sistemas;

vi) įrašai apie tuos informacijos saugumo įvykius, kuriuos gali reikėti iš naujo įvertinti, kad būtų atskleisti neaptikti informacijos saugumo incidentai ar pažeidžiamumas.

2) 1 punkto i papunktyje nurodyti įrašai saugomi bent 5 metus nuo patvirtinimo galiojimo pabaigos.

3) 1 punkto ii papunktyje nurodyti įrašai saugomi bent 5 metus nuo sutarties pakeitimo arba nutraukimo.

4) 1 punkto iii, iv ir v papunkčiuose nurodyti įrašai saugomi bent 5 metus.

5) 1 punkto vi papunktyje nurodyti įrašai saugomi tol, kol tie informacijos saugumo įvykiai bus pakartotinai įvertinti organizacijos nustatytoje tvarkoje numatytu periodiškumu.

b) Organizacija saugo įrašus, susijusius su savo darbuotojų, vykdančių informacijos saugumo valdymo veiklą, kvalifikacija ir patirtimi.

1) Įrašai apie darbuotojų kvalifikaciją ir patirtį saugomi tol, kol asmuo dirba organizacijoje, ir ne trumpiau kaip 3 metus po to, kai asmuo paliko organizaciją.

2) Jei darbuotojai paprašo, jiems suteikiama prieiga prie jų individualių įrašų. Be to, jei prieš palikdami organizaciją jie pateikia prašymą, organizacija jiems pateikia jų individualių įrašų kopiją.

c) Kokiu formatu saugomi įrašai, nurodoma organizacijos tvarkoje.

d) Įrašai saugomi taip, kad būtų užtikrinta jų apsauga nuo pažeidimo, pakeitimo ar vagystės, o informacija prireikus identifikuojama pagal jos slaptumo žymos laipsnį. Organizacija užtikrina, kad įrašai būtų saugomi naudojant priemones, užtikrinančias vientisumą, autentiškumą ir sankcionuotą prieigą.

IS.D.OR.250 Informacijos saugumo valdymo vadovas (ISVV)

a) Organizacija pateikia kompetentingai institucijai informacijos saugumo valdymo vadovą (ISVV) ir, kai taikoma, visus jame minimus susijusius vadovus ir procedūras; tame ISVV pateikiama:

1) atsakingo vadovo arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovo pasirašytas pareiškimas, kuriuo patvirtinama, kad organizacija visais atvejais laikysis šio priedo ir ISVV. Jei atsakingas vadovas arba, projektavimo organizacijų atveju, projektavimo organizacijos vadovas nėra organizacijos generalinis direktorius (CEO), pareiškimą turi pasirašyti generalinis direktorius;

2) IS.D.OR.240 punkto b ir c papunkčiuose nurodyto asmens (-ų) vardas (-ai) ir pavardė (-ės), pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

3) IS.D.OR.240 punkto d papunktyje nurodyto bendro asmens (-ų) vardas (-ai), pavardė (-ės), pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

4) organizacijos informacijos saugumo politika, nurodyta IS.D.OR.200 punkto a papunkčio 1 dalyje;

5) bendras turimų darbuotojų skaičiaus, jų kategorijų bei apsirūpinimo darbuotojais planavimo sistemos, kaip reikalaujama IS.D.OR.240 punkte, aprašymas;

6) pagrindinių asmenų, atsakingų už IS.D.OR.200 punkto įgyvendinimą, įskaitant asmenį (-is), atsakingą (-us) už atitikties stebėsenos funkciją, nurodytą IS.D.OR.200 punkto a papunkčio 12 dalyje, pareigos, atskaitomybė, atsakomybė ir įgaliojimai;

7) organizacijos struktūros schema, kurioje nurodyti susiję 2 ir 6 punktuose nurodytų asmenų atskaitomybės ir atsakomybės ryšiai;

8) vidaus pranešimų teikimo sistemos, nurodytos IS.D.OR.215 punkte, aprašymas;

9) procedūros, kuriomis nustatoma, kaip organizacija užtikrina atitiktį šiai daliai, visų pirma:

i) dokumentacija, nurodyta IS.D.OR.200 punkto c papunktyje;

ii) procedūros, kuriomis nustatoma, kaip organizacija kontroliuoja bet kokią pagal sutartį vykdomą veiklą, nurodytą IS.D.OR.200 punkto a papunkčio 9 dalyje;

iii) ISVV pakeitimo procedūra, apibrėžta c punkte;

10) išsami informacija apie esamas patvirtintas alternatyvias atitikties užtikrinimo priemones.

b) Pirminį ISVV išdavimą patvirtina ir ISVV kopiją pasilieka kompetentinga institucija. ISVV, jeigu būtina, turi būti keičiamas siekiant užtikrinti, kad jame visa laiką būtų naujausi duomenys apie organizacijos ISVS. Visų ISVV pakeitimų kopijos pateikiamos kompetentingai institucijai.

c) ISVV pakeitimai tvarkomi organizacijos nustatyta tvarka. Visus pakeitimus, kurie nepatenka į šios procedūros taikymo sritį, ir visus pakeitimus, susijusius su IS.D.OR.255 punkto b papunktyje nurodytais pakeitimais, tvirtina kompetentinga institucija.

d) Organizacija gali integruoti ISVV su kitais savo turimais valdymo žinynais ar vadovais, jei yra aiški kryžminė nuoroda, kurios valdymo žinyno ar vadovo dalys atitinka įvairius šiame priede nustatytus reikalavimus.

IS.D.OR.255 Informacijos saugumo valdymo sistemos pakeitimai

a) ISVS pakeitimai gali būti administruojami ir apie juos gali būti pranešama kompetentingai institucijai pagal organizacijos parengtą procedūrą. Šią procedūrą tvirtina kompetentinga institucija.

b) Dėl ISVS pakeitimų, kuriems netaikoma a punkte nurodyta procedūra, organizacija kompetentingai institucijai turi pateikti prašymą dėl patvirtinimo ir jį gauti.

Dėl šių pakeitimų:

1) prašymas pateikiamas prieš įgyvendinant tokį pakeitimą, kad kompetentinga institucija galėtų nustatyti, ar tebesilaikoma šio reglamento, ir, jei reikia, iš dalies pakeisti organizacijos pažymėjimą ir atitinkamas prie jo pridėto patvirtinimo sąlygas;

2) organizacija pateikia kompetentingai institucijai visą informaciją, kurios ji prašo pakeitimui įvertinti;

3) pakeitimas įgyvendinamas tik gavus oficialų kompetentingos institucijos patvirtinimą;

4) tokių pakeitimų įgyvendinimo metu organizacija veikia kompetentingos institucijos nustatytomis sąlygomis.

IS.D.OR.260 Tęstinis tobulinimas

a) Organizacija, naudodama tinkamus veiklos rezultatų rodiklius, įvertina ISVS veiksmingumą ir brandumą. Tas vertinimas atliekamas pagal organizacijos iš anksto nustatytą grafiką arba po informacijos saugumo incidento.

b) Jei atlikus vertinimą pagal a punktą nustatoma trūkumų, organizacija imasi būtinų tobulinimo priemonių, siekdama užtikrinti, kad ISVS toliau atitiktų taikomus reikalavimus ir padėtų išlaikyti priimtiną informacijos saugumo rizikos lygį. Be to, organizacija iš naujo įvertina tuos ISVS elementus, kuriems padarė poveikį priimtos priemonės.