

**Pieņemami atbilstības nodrošināšanas līdzekļi un vadlīnijas par Komisijas Īstenošanas regulas (ES) 2023/203 II pielikumu (IS.I.OR daļu)**

1. izdevums

2023. gada 12. jūlijā[[1]](#footnote-2)

# SATURA RĀDĪTĀJS

[SATURA RĀDĪTĀJS 2](#_Toc175135355)

[AMC UN GM PAR KOMISIJAS ĪSTENOŠANAS REGULAS (ES) 2023/203 II PIELIKUMU (IS.I.OR DAĻU) 7](#_Toc175135356)

[GM1 par IS.I.OR.200. punktu “Informācijas drošības pārvaldības sistēma (IDPS)” 7](#_Toc175135357)

[AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 1) daļu 12](#_Toc175135358)

[GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 1) daļu 13](#_Toc175135359)

[AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 12) daļu 14](#_Toc175135360)

[GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 12) daļu 14](#_Toc175135361)

[AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 13) daļu 14](#_Toc175135362)

[AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” c) apakšpunktu 14](#_Toc175135363)

[GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” c) apakšpunktu 15](#_Toc175135364)

[GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” d) apakšpunktu 16](#_Toc175135365)

[AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” e) apakšpunktu 17](#_Toc175135366)

[GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” e) apakšpunktu 17](#_Toc175135367)

[GM1 par IS.I.OR.205. punktu “Informācijas drošības riska novērtējums” 18](#_Toc175135368)

[AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” a) apakšpunktu 18](#_Toc175135369)

[GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” a) apakšpunktu 18](#_Toc175135370)

[AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu 19](#_Toc175135371)

[GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu 19](#_Toc175135372)

[GM2 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu 20](#_Toc175135373)

[AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” c) apakšpunktu 20](#_Toc175135374)

[GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” c) apakšpunktu 21](#_Toc175135375)

[AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu 26](#_Toc175135376)

[GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu 26](#_Toc175135377)

[GM2 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu 27](#_Toc175135378)

[AMC1 par IS.I.OR.205. punkta e) apakšpunktu “Informācijas drošības riska novērtējums” 28](#_Toc175135379)

[GM1 par IS.I.OR.205. punkta e) apakšpunktu “Informācijas drošības riska novērtējums” 28](#_Toc175135380)

[GM1 par IS.I.OR.210. punktu “Informācijas drošības riska risināšana” 30](#_Toc175135381)

[AMC1 par IS.I.OR.210. punkta “Informācijas drošības riska risināšana” a) apakšpunktu 31](#_Toc175135382)

[AMC1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 31](#_Toc175135383)

[GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 32](#_Toc175135384)

[GM2 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 32](#_Toc175135385)

[GM3 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 32](#_Toc175135386)

[GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” c) apakšpunktu 33](#_Toc175135387)

[GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” d) apakšpunktu 33](#_Toc175135388)

[GM1 par IS.I.OR.220. punktu “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” 34](#_Toc175135389)

[AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” a) apakšpunktu 34](#_Toc175135390)

[GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” a) apakšpunktu 34](#_Toc175135391)

[AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) apakšpunktu 35](#_Toc175135392)

[GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) apakšpunktu 36](#_Toc175135393)

[AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” c) apakšpunktu 36](#_Toc175135394)

[GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) un c) apakšpunktu 37](#_Toc175135395)

[GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” c) apakšpunktu 38](#_Toc175135396)

[AMC1 par IS.I.OR.225. punktu “Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem” 39](#_Toc175135397)

[GM1 par IS.I.OR.225. punktu “Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem” 39](#_Toc175135398)

[GM1 par IS.I.OR.230. punktu “Sistēma ārējai ziņošanai par informācijas drošību” 39](#_Toc175135399)

[AMC1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 40](#_Toc175135400)

[GM1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” a) un b) apakšpunktu 40](#_Toc175135401)

[AMC1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” c) apakšpunktu 41](#_Toc175135402)

[GM1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” c) apakšpunktu 42](#_Toc175135403)

[GM1 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana” 42](#_Toc175135404)

[GM2 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana” 42](#_Toc175135405)

[GM3 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana” 43](#_Toc175135406)

[AMC1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu 45](#_Toc175135407)

[GM1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu 46](#_Toc175135408)

[GM2 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu 47](#_Toc175135409)

[AMC1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana” b) apakšpunktu 47](#_Toc175135410)

[GM1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana” b) apakšpunktu 47](#_Toc175135411)

[GM1 par IS.I.OR.240. punktu “Prasības personālam” 47](#_Toc175135412)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 2) daļu 48](#_Toc175135413)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 3) daļu 48](#_Toc175135414)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 3) daļu 48](#_Toc175135415)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” b) apakšpunktu 48](#_Toc175135416)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” b) apakšpunktu 49](#_Toc175135417)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” b) un c) apakšpunktu 49](#_Toc175135418)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” c) apakšpunktu 49](#_Toc175135419)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” d) apakšpunktu 49](#_Toc175135420)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” e) apakšpunktu 49](#_Toc175135421)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” f) apakšpunktu 50](#_Toc175135422)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” f) apakšpunktu 50](#_Toc175135423)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” g) apakšpunktu 50](#_Toc175135424)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” g) apakšpunktu 51](#_Toc175135425)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” h) apakšpunktu 51](#_Toc175135426)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” h) apakšpunktu 52](#_Toc175135427)

[AMC1 par IS.I.OR.240. punkta “Prasības personālam” i) apakšpunktu 52](#_Toc175135428)

[GM1 par IS.I.OR.240. punkta “Prasības personālam” i) apakšpunktu 52](#_Toc175135429)

[GM1 par IS.I.OR.245. punktu “Reģistrācija” 53](#_Toc175135430)

[AMC1 par IS.I.OR.245. punkta “Reģistrācija” a) apakšpunkta 1) daļas vi) punktu un a) apakšpunkta 5) daļu 53](#_Toc175135431)

[GM1 par IS.I.OR.245. punkta “Reģistrācija” a) apakšpunkta 1) daļas vi) punktu un a) apakšpunkta 5) daļu 53](#_Toc175135432)

[AMC1 par IS.I.OR.245. punkta “Reģistrācija” c) un d) apakšpunktu 54](#_Toc175135433)

[GM1 par IS.I.OR.245. punkta “Reģistrācija” c) un d) apakšpunktu 54](#_Toc175135434)

[GM1 par IS.I.OR.250. punkta “Informācijas drošības pārvaldības rokasgrāmata (IDPR)” a) apakšpunktu 55](#_Toc175135435)

[AMC1 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas” 55](#_Toc175135436)

[GM1 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas” 56](#_Toc175135437)

[GM2 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas” 56](#_Toc175135438)

[AMC1 par IS.I.OR.260. punktu “Pastāvīgi uzlabojumi” 57](#_Toc175135439)

[GM1 par IS.I.OR.260. punktu “Pastāvīgi uzlabojumi” 58](#_Toc175135440)

[AMC1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” a) apakšpunktu 59](#_Toc175135441)

[GM1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” a) apakšpunktu 60](#_Toc175135442)

[AMC1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” b) apakšpunktu 62](#_Toc175135443)

[GM1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” b) apakšpunktu 62](#_Toc175135444)

[I papildinājums 64](#_Toc175135445)

[Piemēri apdraudējumu scenārijiem, kam var būt nelabvēlīga ietekme uz drošumu 64](#_Toc175135446)

[II papildinājums 71](#_Toc175135447)

[Galvenie uzdevumi, kas izriet no *IS* daļas ieviešanas, tostarp atbilstība *NIST CSF* 71](#_Toc175135448)

[1.1. versijas kompetencēm un ISO/IEC 27001 punktiem un kontroles pasākumiem 71](#_Toc175135449)

[III papildinājums 79](#_Toc175135450)

[Aviācijas pakalpojumu piemēri 79](#_Toc175135451)

# *AMC* UN *GM* PAR KOMISIJAS ĪSTENOŠANAS REGULAS (ES) 2023/203 II PIELIKUMU (IS.I.OR DAĻU)

## GM1 par IS.I.OR.200. punktu “Informācijas drošības pārvaldības sistēma (IDPS)”

**Informācijas drošības pārvaldības sistēma (IDPS)** ir sistemātiska pieeja organizācijas informācijas drošības stāvokļa noteikšanai, ieviešanai, vadīšanai, uzraudzīšanai, pārskatīšanai, uzturēšanai un pastāvīgai uzlabošanai. Tās mērķis ir aizsargāt informācijas aktīvus, lai varētu efektīvi un iedarbīgi sasniegt organizācijas darbības un drošuma mērķus, apzinoties riskus.

Vispārīgi runājot, ar IDPS tiek izveidots informācijas drošības riska pārvaldības process, pamatojoties uz tādas informācijas drošības ietekmes analīzes rezultātiem, kas būtībā nosaka tās tvērumu. Ja informācijas drošības pārkāpumi var radīt vai veicināt nelabvēlīgu ietekmi uz aviācijas drošumu, ar informācijas drošības prasībām ir jāierobežo to ietekme uz aviācijas drošuma līmeņiem, kuri tiek uzskatīti par pieņemamiem. Līdz ar to Regulas (ES) 2023/203 darbības jomā ietilpst visas funkcijas, procesi vai informācijas sistēmas, kas var radīt vai veicināt nelabvēlīgu ietekmi uz aviācijas drošumu. IDPS nodrošina līdzekļus lēmuma pieņemšanai par nepieciešamo informācijas drošības kontroli visos arhitektūras slāņos (pārvaldība, darbība, piemērošana, tehnoloģijas, dati) un sfērās (organizatoriskā, cilvēciskā, fiziskā, tehniskā sfēra). Tā arī ļauj pārvaldīt informācijas drošības kontroles pasākumu atlasi, ieviešanu un izmantošanu. Visbeidzot, ar to var vadīt pārvaldības, riska pārvaldības un atbilstības (*GRC*) darbības IDPS tvērumā.

Tādējādi riska pārvaldības procesa pamatā ir aviācijas drošuma riska novērtējumi un atvasināti informācijas drošības riska pieņemšanas līmeņi, kas izstrādāti, lai efektīvi risinātu un pārvaldītu informācijas drošības riskus, kuri var ietekmēt aviācijas drošumu un kurus rada apdraudējums, kas saistīts ar aeronavigācijas sistēmu informācijas aktīvu ievainojamībām. Mijiedarbības tauriņveida diagrammas ļauj neizsmeļoši atspoguļot augstākā līmenī to, kāda sadarbība var būt nepieciešama starp dažādām riska novērtēšanas disciplīnām, lai izveidotu kopīgu riska perspektīvu, kā parādīts 1. attēlā.

****

**1. attēls. Informācijas drošības apdraudējumu radīto aviācijas drošuma risku pārvaldības tauriņveida attēlojums**

Šajā regulā aprakstītajā informācijas drošības pārvaldības sistēmā (IDPS) ir jāapvieno informācijas drošības un aviācijas drošuma kompetences lielākajā daļā procesu, tostarp, piemēram, nosakot kritiskās sistēmas vai apdraudējumu un novērtējot iespējamo ietekmi uz aviācijas drošumu un riskus aviācijas drošumam.

**IDPS ieviešana un uzturēšana**

Šajā regulā noteiktajā IDPS ir izmantotas pārvaldības, riska un atbilstības perspektīvas un pieeja, kurā apvienotas drošuma risku un darbības rādītāju dimensijas, lai noteiktu konkrētajiem apstākļiem piemērotus un atbilstošus informācijas drošības kontroles pasākumus, ar kuriem var efektīvi nodrošināt aviācijas drošuma mērķu sasniegšanai nepieciešamo aizsardzības līmeni, kur:

* **pārvaldības** perspektīva attiecas uz pārvaldības un vadības virziena nodrošināšanu, lai sasniegtu struktūras vispārējos mērķus:
* augstākā līmeņa vadības līderība un apņemšanās, kas nosaka un nodrošina ciešu vadības iesaisti un “lejupēju” IDPS ieviešanu;
* informācijas drošības un drošuma mērķi, kas ir saskaņoti ar struktūras darbības mērķiem un atbilst tiem, un tiek uzraudzīti, izmantojot, piemēram, vadības pārskatus;
* informācijas drošības politika, kurā ir noteikti principi un sasniedzamie mērķi;
* funkcijas, pienākumi, kompetences un resursi, kas nepieciešami efektīvai IDPS;
* efektīva, uz mērķgrupām vērsta saziņa ar iekšējām un ārējām ieinteresētajām personām;
* **riska** perspektīva attiecas uz būtisku IDPS aspektu aviācijas drošuma kontekstā atbilstoši šai regulai, un nodrošina pamatu, lai pārredzami pieņemtu lēmumus un noteiktu prioritāros kontroles pasākumus un riska risināšanas iespējas. Tā arī attiecas uz informācijas drošības risku novērtēšanu, risināšanu un uzraudzību, lai sekmētu aviācijas drošuma risku pārvaldību attiecībā uz galvenajiem procesiem un informācijas aktīviem, no kuriem tie ir atkarīgi. Tā ietver aizsardzības prasības, pakļautību riskam, attieksmi pret riskiem un riska pieņemšanas kritērijus, metodes un nozares standartus;
* **atbilstības** perspektīva attiecas uz atbilstību reglamentējošajām, tiesiskajām un līgumiskajām prasībām. Tā ietver atbilstību:
* šai regulai;
* struktūras politikai un standartiem un var ietvert arī atbilstību starptautiskajiem vai nozares standartiem, ko struktūra ir pārņēmusi no ISO, *EUROCAE* u. c.

Šī perspektīva ietver nepieciešamo informācijas drošības noteikumu noteikšanu, īstenošanu un uzturēšanu, un to rezultativitāte un ievērošana ir regulāri jāuzrauga un jānodrošina, piemēram, veicot (iekšējas) revīzijas.

Izmantojot minētās perspektīvas, var noteikt turpmāk minētos procesus vai tematiskās jomas, kam, kā pierādīts, ir būtiska nozīme efektīvas IDPS izveidē. IDPS procesus un tematiskās jomas var rezumēt šādi:

a) konteksta noskaidrošana, nosakot tvērumu, saskarnes, atkarības un ieinteresēto personu prasības;

b) augstākā līmeņa vadības līderība un apņemšanās;

c) informācijas drošības un drošuma mērķi;

d) informācijas drošības politika;

e) funkcijas, pienākumi, kompetences un resursi, kas nepieciešami efektīvai IDPS;

f) saziņa ar iekšējām un ārējām ieinteresētajām personām, lai panāktu pietiekamu informētību par informācijas drošību, un visu iesaistīto pušu mācības;

g) informācijas drošības riska pārvaldība, tostarp riska novērtēšana un risināšana;

h) informācijas drošības incidentu pārvaldība, izveidojot procesus informācijas drošības incidentu un ievainojamību apstrādei;

i) darbības rādītāju un rezultativitātes uzraudzība, mērīšana un novērtēšana;

j) iekšējās revīzijas un vadības pārskati;

k) labojumi un korektīvi pasākumi;

l) pastāvīgi uzlabojumi;

m) attiecības ar piegādātājiem;

n) dokumentēšana, reģistrācija un pierādījumu vākšana.

Papildu faktori, kas ir būtiski sekmīgai IDPS ieviešanai un darbībai, ir šādi:

* IDPS ir jāintegrē struktūras procesos un vispārējā pārvaldības struktūrā vai – vismaz daļēji, to attiecīgās integritātes aizsardzības pasākumos un attiecīgā gadījumā – pat visaptverošā vadības sistēmā, kas ietver informācijas drošību, aviācijas drošumu un kvalitātes pārvaldību;
* lai nodrošinātu maksimālu rezultativitāti, minimālu funkcionālu iejaukšanos un optimizētu izmaksas, informācijas drošība ir jāņem vērā procesu un procedūru, sistēmu un informācijas drošības kontroles pasākumu vispārējās izstrādes sākumposmā. Neviens no šiem ieguvumiem nav sasniedzams, ja tā tiek integrēta vēlāk;
* riska pārvaldības process nosaka atbilstošus preventīvu kontroles pasākumu raksturlielumus, lai sasniegtu un uzturētu pieņemamus riska līmeņus;
* incidentu pārvaldības process nodrošina, ka organizācija laikus atklāj informācijas drošības incidentus, rīkojas un reaģē uz tiem; to panāk, iepriekš nosakot pienākumus, procedūras, scenārijus un reaģēšanas plānus, lai nodrošinātu saskaņotu, mērķtiecīgu un efektīvu reaģēšanu;
* reaģējot, notiek pastāvīga uzraudzība un izvērtēšana, un tiek veikti uzlabojumi.

Iepriekšminētie pamatelementi ir saistīti ar šīs regulas prasībām, attiecībā uz kurām 2. attēlā ir sniegts to aspektu augsta līmeņa attēlojums, kuri ir nozīmīgāki ieviešanas posmā, un to, kuri raksturo darbības posmu, kā arī pārskatīšanu un iespējamos uzlabojumus, ja funkcijas nedarbojas, kā plānots.



**2. attēls. *IS* daļas prasību attēlojums no IDPS dzīves cikla perspektīvas**

**“Plānot, darīt, pārbaudīt, rīkoties” pieeja**

“Plānot, darīt, pārbaudīt, rīkoties” (*PDCA*) ir procesa pieeja, ko bieži izmanto, lai noteiktu, ieviestu, ekspluatētu, uzraudzītu, pārskatītu un uzlabotu pārvaldības sistēmas. 3. attēlā parādīta *PDCA* pieejas piemērošana attiecībā uz IDPS.



**3. attēls. “Plānot, darīt, pārbaudīt, rīkoties” pieejas piemērošana attiecībā uz IDPS**

**Ieguvumi no IDPS**

Ieguvumi no pārvaldības sistēmas, kas darbojas dinamiskā, nenoteiktā vai neparedzamā riska vidē, ilgtermiņā tiek panākti tikai tad, ja organizācija uzlabo pašreizējos kontroles pasākumus, procesus un risinājumus, pamatojoties uz risku, darbības rādītāju un gatavības novērtējumu, kā arī uz pieredzi, kas gūta no incidentiem, revīzijām, neatbilstībām un to galvenajiem cēloņiem. IDPS sekmīga pieņemšana un ieviešana ļauj struktūrai:

* uzlabot vadības un ieinteresēto personu pārliecību par to, ka tās informācijas aktīvi ir pastāvīgi un pienācīgi aizsargāti pret apdraudējumu;
* palielināt tās uzticamību, sniedzot ieinteresētajām personām pārliecību par to, ka informācijas drošības riski, kas ietekmē aviācijas drošumu, tiek pienācīgi pārvaldīti;
* palielināt struktūras galveno procesu noturību pret nesankcionētu elektronisku iejaukšanos un saglabāt struktūras spēju pieņemt lēmumus un rīkoties;
* palīdzēt laikus atklāt kontroles trūkumus, ievainojamības vai nepilnības, lai novērstu informācijas drošības incidentus vai vismaz mazinātu to ietekmi;
* atklāt izmaiņas struktūras vidē, tostarp sistēmas arhitektūrā un apdraudējuma ainā vai jaunu tehnoloģiju ieviešanā, un laikus reaģēt uz tām;
* nodrošināt pamatu efektīvai un rentablai vispusīgas informācijas drošības stratēģijas ieviešanai laikā, kad notiek digitālā transformācija, pieaug sistēmu savienojamība, parādās jauni informācijas drošības apdraudējumi un jaunas tehnoloģijas.

**Saistība ar ISO/IEC 27001**

Starptautiskais standarts ISO/IEC 27001 ir plaši pieņemts standarts attiecībā uz IDPS un tajā ir noteiktas vispārējas prasības IDPS izveidei, ieviešanai, uzturēšanai un pastāvīgai uzlabošanai. Tajā ir ietvertas arī prasības attiecībā uz informācijas drošības risku novērtēšanu un risināšanu. Prasības ir piemērojamas visām struktūrām neatkarīgi no to veida, lieluma vai darbības veida. IDPS atbilstību standartam ISO/IEC 27001 var sertificēt akreditēta sertifikācijas iestāde. ISO/IEC 27001 ir saderīgs ar citiem pārvaldības sistēmas standartiem (kvalitāte, drošums utt.), kuros arī ir pārņemta struktūra un termini, kas definēti ISO/IEC direktīvu 1. daļas “Konsolidētais ISO papildinājums” SL pielikumā. Šī saderība ļauj struktūrai izmantot vienotu pārvaldības sistēmu, kas atbilst vairāku pārvaldības sistēmu standartu prasībām.

ISO/IEC 27001 ļauj struktūrām noteikt to revīzijas tvērumu un vēlmi uzņemties organizatoriskos riskus. Tas savukārt nozīmē, ka tiek izvirzītas tādas informācijas drošības prasības, kas nodrošina IDPS informācijas drošības riska pieņemamības kritērijus atbilstoši struktūras vēlmei uzņemties riskus (skat. 4. attēlu).



**4. attēls. Saistība starp struktūras vēlmi uzņemties risku un informācijas drošības mērķiem**

Šajā regulā noteiktās prasības attiecībā uz IDPS lielākoties atbilst ISO/IEC 27001 un ir pielīdzinātas šim standartam; tomēr ar šo regulu tiek ieviesti noteikumi, kas attiecas tieši uz aviācijas drošumu. Ja struktūra citā darbības jomā un apstākļos jau izmanto IDPS, kuras pamatā ir ISO/IEC 27001, to var viegli pielāgot un piemērot šīs regulas darbības jomai un apstākļiem, pamatojoties uz darbības jomas un trūkumu analīzi. Lai nodrošinātu atbilstību *IS* daļai, izmantojot ISO/IEC 27001 sertifikāciju, aviācijas drošumam ir jābūt iekļautam organizatorisko risku pārvaldībā ar attiecīgo riska pieņemamības līmeni, kas noteikts piemērojamajā regulā (skat. 5. attēlu). Tāpēc ir rūpīgi jānosaka IDPS tvērums saistībā ar aviācijas drošuma riskiem, jo tas var atšķirties no tvēruma, kas ir saistīts ar citiem organizatoriskiem riskiem. Lai varētu pierādīt atbilstību Regulai (ES) 2023/203, IDPS aspekti, kas saistīti ar aviācijas drošuma riskiem, var būt rūpīgi jānošķir no citiem organizatoriskiem riskiem. Tas var ietekmēt lēmumu par informācijas drošības pārvaldības sistēmu (IDPS) integrēšanu.



**5. attēls. Aviācijas drošuma aspektu iekļaušana struktūras vēlmē uzņemties risku**

***IS* daļas un ISO/IEC 27001 savstarpējo norāžu tabula**

Informāciju par *IS* daļā noteiktajiem galvenajiem uzdevumiem un atbilstošajiem ISO/IEC 27001 noteikumiem, un saistītajiem kontroles pasākumiem skat. II papildinājumā.

## AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 1) daļu

Organizācijai jānosaka un jādokumentē IDPS tvērums, nosakot darbības, procesus, atbalsta sistēmas un to, kas var ietekmēt aviācijas drošumu.

Informācijas drošības politika jāapstiprina atbildīgajam vadītājam un jāpārskata plānotos intervālos vai tad, ja notiek būtiskas izmaiņas. Turklāt politikā ir jāietver vismaz turpmāk norādītie aspekti ar iespējamu ietekmi uz aviācijas drošumu:

a) apņemšanās izpildīt piemērojamos tiesību aktus, ņemt vērā attiecīgos standartus un labāko praksi;

b) informācijas drošības pārvaldības mērķu un darbības rādītāju noteikšana;

c) organizācijas vispārējo principu, darbību, procesu noteikšana, lai pienācīgi nodrošinātu informācijas un sakaru tehnoloģiju sistēmas un datus;

d) apņemšanās piemērot IDPS prasības organizācijas procesos;

e) apņemšanās pastāvīgi uzlabot informācijas drošības procesa gatavības līmeni saskaņā ar IS.I.OR.260. punktu;

f) apņemšanās izpildīt piemērojamās prasības attiecībā uz informācijas drošību un tās proaktīvu un sistemātisku pārvaldību, kā arī nodrošināt atbilstošus resursus tās īstenošanai un darbībai;

g) jānosaka, ka informācijas drošība ir viens no galvenajiem visu vadītāju pienākumiem;

h) apņemšanās regulāri vai izmaiņu veikšanas gadījumā sekmēt informācijas drošības politiku, organizācijā rīkojot mācības vai informētības palielināšanas sanāksmes visiem darbiniekiem;

i) jāveicina taisnīguma kultūras ieviešana un ziņošana par ievainojamībām, aizdomīgiem / normai neatbilstošiem notikumiem un/vai informācijas drošības incidentiem;

j) apņemšanās attiecīgā gadījumā informēt visas attiecīgās puses par informācijas drošības politiku.

Piezīme. Būtiskas izmaiņas ir ievērojami grozījumi vai pārveidojumi, kas būtiski ietekmē organizācijas darbības, piemēram, strukturālas izmaiņas organizācijā reorganizācijas dēļ, izmaiņas darba procesos (piemēram, darbs no mājām, personīgo ierīču lietošana), tehnoloģiju attīstība (piemēram, dalīti skaitļošanas resursi, mākslīgais intelekts / mašīnmācīšanās) vai apdraudējuma ainas attīstība.

## GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 1) daļu

**INFORMĀCIJAS DROŠĪBAS POLITIKA UN MĒRĶI**

Informācijas drošības politikai jāatbilst organizācijas mērķim un jāvirza savi informācijas drošības pasākumi. Šādā politikā jāietver ar organizāciju saistītās informācijas drošības vajadzības, augsta līmeņa paziņojums par informācijas drošības pasākumu virzienu un nolūku, principi un svarīgākie stratēģiskie un taktiskie mērķi, ko paredzēts sasniegt ar IDPS, kā arī vispārējie informācijas drošības mērķi vai informācijas drošības mērķu noteikšanas sistēmas (kurš, kā) specifikācija. Informācijas drošības politikā jāietver arī izveidotās IDPS apraksts, tostarp funkcijas, pienākumi un atsauces uz politiku un standartiem konkrētos jautājumos.

Informācijas drošības mērķiem jābūt:

* saskanīgiem un saskaņotiem ar informācijas drošības politiku, un tajos jābūt ņemtām vērā piemērojamajām informācijas drošības prasībām, kas izriet no vispārējiem organizācijas mērķiem, un riska novērtēšanas un risināšanas rezultātiem (kas savukārt veicina organizācijas stratēģisko mērķu un informācijas drošības politikas īstenošanu);
* regulāri pārskatītiem, lai nodrošinātu, ka tie ir atjaunināti un joprojām atbilstoši;
* izmērāmiem, ja tas ir praktiski iespējams (lai varētu noteikt, vai mērķis ir sasniegts), jābūt konkrētiem, izmērāmiem, sasniedzamiem, reālistiskiem un ar noteiktu termiņu (*SMART* – specific, measurable, attainable, realistic, timely) un saskaņotiem ar visām iesaistītajām atbildīgajām personām.

Nosakot informācijas drošības mērķus, piemēram, pamatojoties uz vispārējiem organizācijas mērķiem, informācijas drošības prasībām vai riska novērtējumu rezultātiem, jānosaka, kā šie mērķi tiks sasniegti. Tam, cik lielā mērā informācijas drošības mērķi ir sasniegti, jābūt izmērāmam. Ja iespējams, tas jāmēra, izmantojot galvenos darbības rādītājus (*KPI*), kas ir noteikti iepriekš (skat. informatīvos materiālus, piemēram, *COBIT 5* par informācijas drošību). Ieteicams vispirms noteikt ierobežotu skaitu informācijas drošības mērķu, kas ir būtiski organizācijai, attiecas uz ilgāku termiņu un ir izmērāmi, salīdzinot pamatotos centienus ar sniegtajiem ieguvumiem.

## AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 12) daļu

**ATBILSTĪBAS UZRAUDZĪBA**

Nosakot atbilstību IS.I.OR.200. punkta a) apakšpunkta 12) daļai, organizācijai jāīsteno funkcija, lai periodiski uzraudzītu pārvaldības sistēmas atbilstību attiecīgajām prasībām un procedūru piemērotību, tostarp jāizveido iekšējās revīzijas process un informācijas drošības risku pārvaldības process. Ja organizācija jau ir izveidojusi atbilstības uzraudzības funkciju atbilstoši īstenošanas regulai savā sfērā, šādā funkcijā jāietver pārvaldības sistēmas uzraudzība ar atbilstošām prasībām tās darbības ietvaros. Atbilstības uzraudzībā jāiekļauj atgriezeniskās saites mehānisms, lai atbildīgajam vadītājam vai deleģētai(-as) personai(-as) sniegtu atgriezenisko saiti par revīzijas konstatējumiem un vajadzības gadījumā nodrošinātu korektīvu pasākumu īstenošanu.

## GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 12) daļu

**ATBILSTĪBAS UZRAUDZĪBA**

Atbilstības uzraudzības nolūkā iekšējā revīzija jāveic plānotos intervālos, lai vadība varētu pārliecināties par IDPS stāvokli un lai nodrošinātu šādu informāciju:

* IDPS atbilstība šīs regulas prasībām un pašas organizācijas prasībām, kas noteiktas informācijas drošības politikā, procedūrās un līgumos vai kas izriet no informācijas drošības mērķiem vai riska risināšanas procesa rezultātiem;
* IDPS efektīva ieviešana un uzturēšana.

Iekšējā revīzija jāīsteno saskaņā ar neatkarīgu pieeju un pierādījumos balstītu lēmumu pieņemšanas procesu. Turklāt revīzijas programmas izstrādē jāņem vērā attiecīgo procesu nozīmīgums un noteiktie revīzijas kritēriji un tvērums. Jāsaglabā dokumentēta informācija, kas apliecina revīzijas rezultātus, to paziņošanu attiecīgajai vadībai un revīzijas programmu.

## AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” a) apakšpunkta 13) daļu

Nosakot atbilstību IS.I.OR.200. punkta a) apakšpunkta 13) daļas noteikumiem, organizācijai ir jāievieš un jāuztur informācijas drošības kontroles pasākumi, kas ir pietiekami stingri un efektīvi, lai aizsargātu informāciju un nodrošinātu zinātvajadzības principu (t. i., informācija ir pieejama tikai tiem, kam tā nepieciešama pienākumu veikšanai). Tai jāaizsargā informācijas avots saskaņā ar attiecīgajiem Regulas (ES) 2018/1139 noteikumiem. Tai ir jāievēro arī Regulas (ES) Nr. 376/2014 prasības.

## AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” c) apakšpunktu

Nodrošinot atbilstību IS.I.OR.200. punkta c) apakšpunkta noteikumiem, organizācijai:

a) jāsniedz konkrētā informācijas drošības personāla (iekšējā un ārējā) struktūras izklāsts, norādot tā funkcijas un pienākumus. Šo struktūras izklāstu izmantos, lai pārvaldītu un uzturētu IDPS tvērumā iekļautos elementus, un to apstiprinās atbildīgais vadītājs. Organizācijai ik pēc noteikta laika vai būtisku izmaiņu gadījumā jāpārskata struktūras izklāsts (skat. piezīmi, kas sniegta AMC1 par IS.I.OR.200. punkta a) apakšpunkta 1) daļu);

b) jānoskaidro un jākategorizē visas attiecīgās nolīgtās organizācijas, ko izmanto IDPS ieviešanai. Organizācijai jānosaka un jādokumentē procedūras saskarņu pārvaldībai un saskaņošanai starp organizāciju un citām organizācijām, tostarp nolīgtajām organizācijām;

c) jānoskaidro un jānosaka visi galvenie procesi un procedūras, kā arī iekšējās un ārējās ziņošanas shēmas, kas tiks izmantotas, lai nodrošinātu atbilstību šīs regulas mērķiem visā IDPS dzīves ciklā. Organizācija var pielāgot pašreizējos procesus vai procedūras, lai nodrošinātu atbilstību;

d) jānoskaidro un jādokumentē jebkāda cita informācija, kas tiks izmantota, lai nodrošinātu atbilstību šīs regulas mērķiem;

e) izveidojot un atjauninot dokumentēto informāciju, jānodrošina pienācīga tās identifikācija un apraksts (piemēram, nosaukums, datums, autors vai atsauces numurs), kā arī tā jāpārskata un jāapstiprina tās piemērotība un atbilstība;

f) jākontrolē dokumentētā informācija, kas nepieciešama IDPS, lai nodrošinātu, ka tā ir:

1) pieejama un piemērota lietošanai, kur un kad tas ir nepieciešams;

2) pienācīgi aizsargāta (piemēram, pret konfidencialitātes zudumu, neatbilstošu izmantošanu vai integritātes zudumu).

## GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” c) apakšpunktu

Informācijas apjoms, kas jādokumentē, lai nodrošinātu atbilstību šīs regulas mērķiem, dažādās organizācijās var atšķirties dažādu faktoru dēļ, piemēram, lieluma un sarežģītības, vai nepieciešamības nodrošināt saskaņotību ar citiem ieviestiem pārvaldības procesiem. Ņemot vērā dokumentus, kas vajadzīgi, lai izpildītu IS.I.OR.200. punkta a) apakšpunkta prasības, IS.I.OR.245. punktā minētās reģistrācijas prasības un IS.I.OR.250. punktā minētās informācijas drošības pārvaldības rokasgrāmatas prasības, kā vispārīgs norādījums turpmāk ir sniegts neizsmeļošs dokumentējamās informācijas uzskaitījums:

a) informācijas drošības politika, kurā jāiekļauj organizācijas informācijas drošības mērķi (skat. IS.I.OR.200. punkta a) apakšpunkta 1) daļu);

b) ar informācijas drošību saistīto darbinieku pienākumi un pakļautība (skat. IS.I.OR.250. punkta a) apakšpunkta 2), 3), 6) un 7) daļu un personāla prasības, kas minētas IS.I.OR.240. punkta a), b), c), d) un f) apakšpunktā un saistītajos *AMC* un *GM*);

c) IDPS tvērums un saskarnes ar citām pusēm un atkarība no tām – skat. IS.I.OR.200. punkta a) apakšpunkta 2) daļu un informācijas drošības prasības, kas minētas IS.I.OR.205. punkta a) un b) apakšpunktā;

d) informācijas drošības risku pārvaldības process – skat. informācijas drošības prasības, kas minētas IS.I.OR.205. un IS.I.OR.210. punktā;

e) informācijas drošības riska novērtējumā konstatēto risku un saistīto riska risināšanas pasākumu arhīvs (bieži dēvēts par “risku reģistru” vai “risku virsgrāmatu”) – skat. IS.I.OR.245. punktu;

f) pierādījumi par kompetencēm, kas nepieciešamas personālam, kurš veic šajā regulā paredzētās darbības – skat. IS.I.OR.240. punkta g) apakšpunktu un saistītos *AMC* un *GM*;

g) pierādījumi par tā personāla pašreizējām kompetencēm, kuri veic šajā regulā paredzētos pasākumus – skat. IS.I.OR.245. punkta b) apakšpunkta 1) daļu;

h) (galvenie) darbības rādītāji, kas iegūti no pierādījumiem par IDPS procesu uzraudzību un mērīšanu.

## GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” d) apakšpunktu

**SAMĒRĪGUMS IDPS IEVIEŠANĀ**

Ieviešot procesus un procedūras, kā arī nosakot IS.I.OR.200. punkta d) apakšpunktā aprakstītās funkcijas un pienākumus, organizācijai vispirms ir jāņem vērā riski, ko tā var radīt citām organizācijām, kā arī tās pašas pakļautība riskam. Citi aspekti, kas var būt būtiski, ir organizācijas vajadzības un mērķi, informācijas drošības prasības, pašas organizācijas procesi un organizācijas lielums, sarežģītība un struktūra – laika gaitā šie visi aspekti var mainīties.

**ATBALSTĪTA IDPS IEVIEŠANA**

Saistībā ar *IS* daļu visas organizācijas uzsāk IDPS ieviešanu, nosakot tās tvērumu, kas savukārt balstās vismaz uz novērtējumu par tādu ietekmi uz aviācijas drošumu, kuru izraisa vai veicina informācijas drošības incidenti. Organizācijām neatkarīgi no to lieluma vēl var nebūt pietiekamu zināšanu par saviem informācijas drošības riskiem, un tās var apsvērt iespēju lūgt atbalstu pakalpojumu sniedzējam, kas šajā IDPS ieviešanas posmā var nodrošināt arī papildu personālu un speciālās zināšanas. Tas pats var attiekties uz turpmākajiem IDPS ieviešanas posmiem, un šajā nolūkā organizācijas var apsvērt IS.I.OR.235. punktu un saistītos *AMC*. Konkrētu IDPS funkciju, piemēram, informācijas drošības uzraudzības vai reaģēšanas uz incidentiem, nodošana ārpakalpojumu sniedzējiem, var palīdzēt nodrošināt, ka organizācijai ir pieejams pieredzējis personāls un speciālās zināšanas. Tāpat organizācijas var saņemt atbalstu no pakalpojumu sniedzēja riska novērtēšanā.

Attiecībā uz tāda atbilstoša personāla izveidi, kas nepieciešams, lai ieviestu un izpildītu šīs regulas noteikumus, organizācijām vienmēr jāpamatojas uz AMC1 par IS.I.OR.240. punkta f) apakšpunktu un GM1 par IS.I.OR.240. punkta f) apakšpunktu, ievērojot to, ka vienai personai var uzticēt vairākus pienākumus, vienlaikus vienmēr nodrošinot atbilstības uzraudzības neatkarību.

Iepazīstoties ar informācijas drošības risku būtību un to pārvaldību, organizācijas kā sākotnējos norādījumus var izmantot *NIST* starpaģentūru ziņojumu (NISTIR 7621 Rev. 1) “Small Business Information Security: The Fundamentals” [Mazās uzņēmējdarbības informācijas drošība. Pamati].

**ŠAJĀ REGULĀ NOTEIKTĀS IDPS INTEGRĒŠANA PAŠREIZĒJĀS PĀRVALDĪBAS SISTĒMĀS**

Ieviešot IDPS, organizācija var izmantot pašreizējo vadības sistēmu priekšrocības un integrēt IDPS šajās pašreizējās sistēmās.

Integrējot IDPS pašreizējās vadības sistēmās, organizācija var samazināt IDPS ieviešanai un uzturēšanai vajadzīgo ieguldījumu un izmaksas un vienlaikus nodrošināt saskaņotību ar organizācijas vispārējo pārvaldības pieeju un atbilstību tai. Turpmāk sniegts neizsmeļošs uzskaitījums ar iespējamām sinerģijām, kuras var izmantot, integrējot IDPS pašreizējā pārvaldības sistēmā.

* Izmantot pašreizējo politiku un procedūras – organizācija var izmantot savu pašreizējo politiku un procedūras kā IDPS pamatu. Tas var palīdzēt nodrošināt saskanību un līdz minimumam samazināt papildu dokumentācijas nepieciešamību.
* Saskaņot IDPS ar citām pārvaldības sistēmām – organizācija var saskaņot IDPS ar citām pārvaldības sistēmām, piemēram, ar drošuma pārvaldības sistēmām (DPS), lai nodrošinātu, ka IDPS atbilst organizācijas vispārējai pārvaldības pieejai.
* Izmantot pašreizējos riska pārvaldības procesus – organizācija var izmantot savus pašreizējos riska pārvaldības procesus, lai identificētu un novērtētu informācijas drošības riskus, kas var radīt aviācijas drošuma riskus.
* Atkārtoti izmantot pašreizējos kontroles pasākumus – organizācija var atkārtoti izmantot pašreizējos kontroles pasākumus, piemēram, piekļuves kontroles pasākumus vai incidentu pārvaldības procesu, lai ieviestu IDPS nepieciešamos informācijas drošības kontroles pasākumus.
* Pastāvīgu uzlabojumu process – organizācija var izmantot pašreizējo pārvaldības sistēmu pastāvīgu uzlabojumu procesu, lai laika gaitā uzlabotu IDPS.

## AMC1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” e) apakšpunktu

**ATKĀPE**

Organizācijām jāievēro norādījumi, kas ir sniegti AMC1 par IS.I.OR.205. punkta a) apakšpunktu un AMC1 par IS.I.OR.205. punkta b) apakšpunktu, lai veiktu dokumentētu informācijas drošības riska novērtējumu nolūkā lūgt kompetentajai iestādei apstiprināt atkāpi saskaņā ar IS.I.OR.200. punkta e) apakšpunktu. Lai pamatotu atkāpi, riska novērtējumā jāsniedz paskaidrojumi par visu elementu izslēgšanu no IDPS tvēruma. Iestāde nosaka, vai šis novērtējums ir apmierinošs, lai varētu atļaut atkāpes piemērošanu.

Organizācijām, kas vēlas, lai riska novērtējumu veic trešā persona, jāņem vērā prasības, kas noteiktas IS.I.OR.235. punktā un saistītajos *AMC*.

## GM1 par IS.I.OR.200. punkta “Informācijas drošības pārvaldības sistēma (IDPS)” e) apakšpunktu

Jebkura organizācija, kas uzskata, ka tā nerada ne sev, ne citai organizācijai nekādu informācijas drošības risku, kurš varētu ietekmēt aviācijas drošumu, var apsvērt iespēju lūgt kompetentajai iestādei atļauju piemērot atkāpi atbilstoši procedūrai, kas izklāstīta AMC1 par IS.I.OR.200. punkta e) apakšpunktu.

Daži piemēri organizācijām, kas var apsvērt iespēju lūgt atkāpi:

* gaisa pārvadātājs, kas veic ar augstu risku nesaistītas specializētas komerciālas darbības (*SPO*), izmantojot vienkāršus lidaparātus, ja darbību raksturs pamato atkāpes piešķiršanu;
* gaisa pārvadātājs, kas ekspluatē ELA2 lidaparātu, kā noteikts Regulas (ES) Nr. 748/2012 1. panta 2. punkta j) apakšpunktā, izņemot lidaparātu, kurš tiek ekspluatēts iepriekš noteiktos ekspluatācijas apstākļos vai ar noteiktiem ekspluatācijas ierobežojumiem;
* tehniskās apkopes organizācija, kas apstiprināta saskaņā ar 145. daļu un kas veic tikai tādu komponentu tehnisko apkopi vai tehniskās apkopes darbības, kuras neveicina lidaparāta strukturālās integritātes nodrošināšanu, un neveic būtiskas ar drošību saistītas funkcijas, bet, piemēram, veic tādas darbības kā mazgāšana, pārklājumu noņemšana, krāsošana utt.

Iepriekšminēto piemēru saraksts nav pilnīgs un tikai norāda uz iespējamajiem scenārijiem, kas varētu būt sākotnējais pamats tāda informācijas drošības riska novērtējuma sagatavošanai, ar kuru tiek pamatota visu organizācijas elementu izslēgšana no IDPS tvēruma.

## GM1 par IS.I.OR.205. punktu “Informācijas drošības riska novērtējums”

*IS* daļā nav noteikts, ka riska novērtējuma izstrādei vai vispārīgai riska pārvaldības īstenošanai ir jāizmanto konkrēta informācijas drošības sistēma, piemēram, ISO, *NIST* vai cita. Katrai sistēmai ir atšķirīgas priekšrocības, un neviena no tām nav ideāli piemērota atsevišķai organizācijai, un tā ir jāpielāgo organizācijas vispārējām vajadzībām, kā arī konkrētai vajadzībai – ņemt vērā aviācijas drošuma aspektus.

Organizācijas, kuru informācijas drošības sistēmām ir piešķirta nozares sertifikācija, var sniegt šo informāciju kā atbalsta informāciju; tomēr šīm organizācijām jāpierāda nozares sertifikācijas piemērojamība šīs regulas darbības jomai (skat. GM1 par IS.I.OR.200. punktu).

Vispārēji norādījumi par riska pārvaldību, tostarp par riska novērtējumu, sniegti standartā ISO/IEC 27005 un ISO/IEC 31000, kā arī NIST SP 800-30. Aviācijas organizācijas var arī apsvērt ar aviāciju saistītus norādījumus, kas sniegti *EUROCAE* dokumenta ED-201A jaunākās redakcijas nodaļā par riska pārvaldību un, atkarībā no konkrētas darba vides, *EUROCAE* dokumenta ED-204A, *EUROCAE* dokumenta ED-205A un *EUROCAE* dokumenta ED-206 nodaļās par riska pārvaldību.

## AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” a) apakšpunktu

Veicot informācijas drošības riska novērtējumu, organizācijai jānodrošina, ka visi attiecīgie aviācijas drošuma elementi tiek noskaidroti un iekļauti IDPS tvērumā atbilstoši IS.I.OR.200. punktam un saistītajiem *AMC*.

Lai nodrošinātu atbilstību IS.I.OR.205. punkta a) apakšpunkta prasībām, var veikt iepriekšēju augsta līmeņa riska novērtējumu vai ietekmes novērtējumu saskaņā ar dokumentētu metodoloģiju un atbilstoši precīziem kritērijiem, lai IDPS tvērumā iekļautu un izslēgtu no tā elementus, kas ir uzskaitīti IS.I.OR.205. punkta a) apakšpunktā.

## GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” a) apakšpunktu

**TVĒRUMA UN ROBEŽU NOTEIKŠANA**

Organizācijai jāveido skaidra un vispusīga izpratne par saviem aviācijas pasākumiem un pakalpojumiem, saistītajiem procesiem un saistītajām informācijas sistēmām, kā arī attiecīgajām datu plūsmām un informācijas apmaiņu, kas nosaka IDPS tvērumu un riska novērtējuma robežas. Tāpēc organizācijai jāizstrādā atbilstoša dokumentācija par resursiem un atkarībām, kas ir saistītas ar skaitļošanu, tīklu veidošanu un nolīgtajiem pakalpojumiem, kuri var ietekmēt riska novērtējuma tvērumā iekļautās informācijas drošību un funkciju, pakalpojumu vai spēju drošumu.

Turpmāk sniegts neizsmeļošs uzskaitījums, kurā sniegti to elementu piemēri, ko var ņemt vērā, lai noteiktu iepriekš minēto tvērumu un robežas. Analīzes detalizācijas pakāpe var būt iteratīvs process ar paredzamajam riska līmenim atbilstošu ieguldīto darbu. Kā minēts iepriekš, mērķis ir panākt izpratni par visiem būtiskajiem aktīviem, resursiem un atkarībām, kas tieši ietilpst funkcijās, pakalpojumos un spējās, veicot šādus pasākumus:

a) organizācijas funkcijām, pakalpojumiem un spējām būtiskās operatīvās ievades un izvades noteikšana; šāda ievade un izvade var būt saistīta ar:

* iekšējiem vai ārējiem avotiem;
* iekšējiem vai ārējiem nomātiem vai pārvaldītiem pakalpojumiem vai citām atkarībām;

b) visu tādu būtisko aktīvu (t. i., aparatūras, programmatūras, tīkla un skaitļošanas resursu) noteikšana, ko izmanto, lai izveidotu, apstrādātu, nosūtītu, uzglabātu vai saņemtu iepriekš minēto operatīvo ievadi un izvadi;

c) visu attiecīgo aktīvu darbības vides (piemēram, biroja, publiskās zonas, ierobežotas pieejamības telpas utt.) un atrašanās vietu noteikšana;

d) attiecībā uz katru tvērumā iekļauto aktīvu nosaka konkrētas metodes, procesus un resursus, kas tiks izmantoti katra aktīva pārvaldīšanai, izmantošanai un uzturēšanai visā tā dzīves ciklā, tostarp:

* iekšējie vai nolīgtie resursi;
* nolīgtie uzņēmumi, kas attālināti pārvalda aktīvus (t. i., pārvaldīto pakalpojumu sniedzējs).

## AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu

Informācijas drošības riska novērtējumā organizācijai jānosaka tās saskarnes ar citām pusēm, piemēram, ar pakalpojumu sniedzējiem, piegādes ķēdēm un citām trešajām personām, pamatojoties uz datu un informācijas apmaiņu un šai apmaiņai izmantotajiem aktīviem, kas varētu radīt situāciju, kad informācijas drošības riski, apdraudot abas puses, var:

* palielināt aviācijas drošuma riskus citām pusēm un/vai
* palielināt aviācijas drošuma riskus pašai organizācijai.

## GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu

**RISKA INFORMĀCIJAS APMAIŅA**

Saskarorganizācijām [organizācijām ar kopīgu saskarni] ir savstarpēji jāapmainās ar informāciju par iespējamajiem informācijas drošības riskiem, piemēram, ievērojot *EUROCAE* dokumenta ED-201A B papildinājuma B.1., B.2. un B.3. punktā izklāstīto pieeju. Šīs informācijas apmaiņas mērķis ir ļaut organizācijām izveidot saskanīgu kartējumu pakalpojumiem, kas norādīti IS.I.OR.205. punkta a) apakšpunktā, tostarp visai informācijai un datu plūsmām, lai:

a) attēlotu (piemēram, izmantojot funkcionālo shēmu) saistību starp loģiskajiem un fiziskajiem ceļiem, kas savieno dažādas iesaistītās daļas;

b) skaidri noteiktu visus aktīvus (t. i., aparatūru, programmatūru, tīkla un skaitļošanas resursus), kas tiks izmantoti apmaiņā;

c) noteiktu visas funkcijas, pasākumus un procesus, tostarp to attiecīgo informāciju un datus, kas tiks izveidoti, nosūtīti, apstrādāti, saņemti un uzglabāti, un saistītu tos ar atbildīgo pusi, kura nodrošina vai veic šīs funkcijas, pasākumus un procesus;

d) attiecībā uz šiem ceļiem, kas veido tā dēvētās funkcionālās ķēdes, noteiktu saskarpuses funkciju, piemēram, vai tā ir attiecīgās informācijas vai datu ģenerētājs, apstrādātājs, sūtītājs vai patērētājs;

e) noteiktu, vai viena saskarpuse šādā ceļā darbojas kā plūsmas iniciators vai kā plūsmas saņēmējs.

**DIVAS SASKARORGANIZĀCIJU KATEGORIJAS**

Ir divas saskarorganizāciju kategorijas, proti, tās, uz kurām attiecas Regula (ES) 2023/203 vai Regula (ES) 2022/1645, un tās, uz kurām šīs regulas neattiecas.

Ja organizācijai ir saskarnes ar organizāciju, uz kuru attiecas Regula (ES) 2023/203 vai Regula (ES) 2022/1645, tad katra struktūra:

* atbild par to saskarņu noteikšanu, kas tās organizācijai ir ar citām organizācijām un kas varētu radīt abpusēju pakļautību informācijas drošības riskiem. Struktūra var gūt labumu no riska informācijas apmaiņas, jo šāda apmaiņa ļauj precīzāk novērtēt šos riskus;
* ir atbildīga par informācijas drošības risku pienācīgu pārvaldību savas IDPS tvērumā.

Visos pārējos gadījumos organizācija ir atbildīga par to informācijas drošības risku pienācīgu pārvaldību, kuri var rasties no tās saskarnes ar otru struktūru. Ja šie riski ir jārisina, organizācijai vienmēr ir iespēja īstenot riska mazināšanas pasākumus un kontroles pasākumus savās robežās. Ja saskarstruktūra ir piegādātājs, organizācija var nolemt risku pārvaldībai izmantot līgumiskas vienošanās un pieprasīt, lai piegādātājs viņa organizācijā īsteno mazināšanas un kontroles pasākumus.

## GM2 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” b) apakšpunktu

**AVIĀCIJAS PAKALPOJUMU PIEMĒRI**

Piemēri aviācijas pakalpojumiem, kurus var apsvērt, nosakot IDPS tvērumu un saskarnes, ir sniegti III papildinājumā.

## AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” c) apakšpunktu

Organizācijai jāizmanto riska pārvaldības sistēma, kurā ietilpst metodoloģija, lai riskiem piešķirtu riska līmeni un noteiktu riska pieņemšanas kritērijus vai turpmāku apstrādi.

Organizācijai jāsniedz dokumentēti pierādījumi par tādu risku novērtējumu, kas var ietekmēt aviācijas drošumu, tostarp par risku līmeni. Organizācijai katrs risks ir jāsaista ar attiecīgajiem elementiem un saskarnēm, kas noteiktas saskaņā ar IS.I.OR.205. punkta a) un b) apakšpunktu, un jādokumentē, vai risks ir pieņemams vai arī tam nepieciešama turpmāka apstrāde.

Organizācijai, dokumentējot šo procesu un tā noturīgumu, jānodrošina pārliecība, ka riska novērtēšanas process tiek veikts ar nepieciešamo stingrību un disciplīnu. To darot, organizācijai ir jāņem vērā:

a) novērtējuma rezultātu reproducējamība līdzīgas ievades gadījumā;

b) novērtējuma atkārtojamība laika gaitā tā, lai dažādo iepriekšējo novērtējumu rezultātus varētu salīdzināt nolūkā noteikt izmaiņas;

c) būtisku un derīgu ievaddatu vākšana, jo īpaši šādas informācijas vākšana:

1) informācija, kas ļauj noteikt ietekmi uz drošumu;

2) informācija, kas ļauj noteikt apdraudējuma scenārija īstenošanās iespējamību;

d) iteratīvi precizējumi laika gaitā, kas, kļūstot pieejamiem ievaddatiem, ļauj izstrādāt precīzākus apdraudējuma scenārijus, lai mazinātu nenoteiktību attiecībā uz apdraudējumu, ievainojamību, spēkā esošo kontroles pasākumu rezultativitāti un atkarību no ārējām struktūrām, jo īpaši:

1) iegūstot vairāk datu, precizēt sākotnējos augsta līmeņa apdraudējuma scenārijus ar lielāku detalizācijas pakāpi un konkrētību;

2) precizēt datus par zināmajām ievainojamībām, pastāvīgi atjauninot informāciju par to izmantojamību un saistītajām sekām;

3) izvērtēt spēkā esošo kontroles pasākumu rezultativitāti un apsvērt jaunos pieejamos kontroles pasākumus;

4) uzlabot izpratni par atkarību no ārējām struktūrām un to ietekmi uz organizācijas riska profilu.

## GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” c) apakšpunktu

**RISKA NOVĒRTĒŠANA**

Turpmāk uzskaitītos riska klasifikācijas līmeņus var piemērot attiecībā uz apdraudējuma scenārija īstenošanās iespējamību un to, cik smagi tā sekas ietekmētu drošumu; tomēr tas neliedz organizācijai izstrādāt papildu starpkategorijas, ja tā uzskata to par vajadzīgu riska novērtējumiem. Organizācijai ir jānorāda un jādokumentē piemērotie, organizācijas lietotie klasifikācijas līmeņi un kvalitatīvi vai kvantitatīvi jānosaka precīzs skaitlisko vērtību diapazons vai intervāls, lai nodrošinātu pietiekami kalibrētu, saskanīgu aplēsi, izvērtējumu un saziņu organizācijā vai ar saskarstruktūrām. Apdraudējuma scenārija īstenošanās iespējamību var izteikt kā iespējamību intervālu, ietverot novērošanas ilgumu. Atbalsta dokumenti un metodes ir pieejamas *EUROCAE* dokumenta ED-203A 3.6. nodaļā, kur ir sniegta atsauce uz apdraudējuma scenārija īstenošanās iespējamības izvērtējumu *EUROCAE* dokumentā ED-202A sniegtajā drošības riska novērtējumā.

1. piezīme. Frāze “novērošanas ilgums” attiecas uz laika posmu, kurā apdraudējuma scenārijs tiek novērots vai uzraudzīts. Tas ir būtiski, lai noteiktu apdraudējuma scenārija īstenošanās iespējamību, jo īstenošanās varbūtība var mainīties atkarībā no novērošanas perioda ilguma.

2. piezīme. *EUROCAE* dokuments ED-202A un *EUROCAE* dokuments ED-203A sākotnēji tika izstrādāti lidaparātu informācijas drošības riska novērtēšanai, bet šajos dokumentos izstrādātos vispārējos principus var pielāgot citām sistēmām, ja organizācija tos uzskata par lietderīgiem.

Lai veicinātu riska novērtēšanas metožu savstarpēju salīdzināmību starp saskarorganizācijām, organizācija var saistīt apdraudējuma scenārija īstenošanās potenciāla novērtējumu ar vienu no šādām kategorijām:

* augsta īstenošanās iespējamība – apdraudējuma scenārijs, visticamāk, īstenosies. Ar apdraudējuma scenāriju saistītais uzbrukums ir ticams, un līdzīgi apdraudējuma scenāriji iepriekš ir daudzkārt īstenojušies;
* vidēja īstenošanās iespējamība – apdraudējuma scenārijs, visticamāk, neīstenosies. Ar apdraudējuma scenāriju saistītais uzbrukums ir iespējams, un iepriekš var būt īstenojies līdzīgs apdraudējuma scenārijs;
* zema īstenošanās iespējamība – apdraudējuma scenārija īstenošanās iespējamība ir ļoti zema. Apdraudējuma scenārija īstenošanās teorētiski ir iespējama, tomēr nav zināms, ka tas būtu noticis.

Apdraudējuma scenārija īstenošanās iespējamības izvērtējumu var balstīt uz turpmāk norādītajiem aspektiem.

**Aizsardzība** (kā noteikts *EUROCAE* dokumentā ED-203A):

* drošības pasākumi un arhitektūra, kas liedz piekļuvi aktīviem – tas, cik lielā mērā aktīvam var piekļūt no kompromitētām sistēmām;
* drošības pasākumu pieejamība – tas, cik lielā mērā drošības pasākums novērš savu pieejamību / uzbrukumu sev no kompromitētām sistēmām;
* mehānisma atteice – tas, cik lielā mērā zināmā drošības pasākuma ieviešana nespēs novērst uzbrukumu;
* atklāšanas metodes vai procedūras uzbrukuma atpazīšanai un atbilstošai reaģēšanai, lai samazinātu apdraudējuma scenārija īstenošanās iespējamību.

**Pakļautības riskam mazināšana** (kā noteikts *EUROCAE* dokumentā ED-203A):

* apstākļi, kuros lietotājs vai uzbrucējs var izmantot ārējas piekļuves savienojumu;
* ārējas piekļuves savienojuma funkcionalitātes ierobežojumi;
* organizatoriskie politikas pasākumi, ar kuriem kontrolē laika, kas vajadzīgs, lai izstrādātu uzbrukuma rīkus konkrētam produktam, attiecību pret šāda rīka izstrādes iespējamību;
* ievainojamību pārvaldība, tostarp izlūkdatu vākšana, skenēšana, risināšana un atkārtota pārbaude, lai ātri un ar augstu pārliecību atklātu, konstatētu un risinātu paziņotās vai atklātās ievainojamības, nosakot riska prioritātes, un tādējādi samazinātu uzbrukuma tvērumu;
* sekmīga uzbrukuma smaguma pakāpes mazināšana (t. i., izmantojot rezerves sistēmu, kas var saglabāt pakalpojuma nepārtrauktību aviācijas drošumam kritiski svarīgas sistēmas darbības atteices gadījumā).

**Uzbrukuma mēģinājums** (kā noteikts *EUROCAE* dokumentā ED-203A):

* uzbrucēju spēja, ko nosaka uzbrukumam nepieciešamie resursi un speciālās zināšanas.

Uzbrucēju spēju var novērtēt vairākos veidos, piemēram, izmantojot:

* informāciju no datortrauksmes reaģēšanas komandām (*CERT*) / datoru drošības incidentu reaģēšanas vienībām (*CSIRT*), informācijas apmaiņas un analīzes centriem (*ISAC*);
* iepriekšējo pasākumu, paņēmienu un procedūru (*TTP*) analīzi un uzbrukumu izdošanās līmeni.

Šā paša iemesla dēļ organizācija ietekmes uz drošumu smaguma pakāpes izvērtējuma rezultātus var saistīt ar vienu no šādām kategorijām:

* augsta smaguma pakāpe – tie tūlītējie vai aizkavētie scenāriji, kas var izraisīt vai veicināt nedrošu stāvokli, ar nedrošu stāvokli saprotot ar lidaparāta ekspluatāciju saistītu notikumu, kurā:
* persona ir gājusi bojā vai guvusi smagus ievainojumus:
* lidaparāts ir guvis bojājumus, vai tiek bojāta tā konstrukcija;
* lidaparāts ir pazudis vai nonācis pilnīgi nepieejamā vietā;
* vidēja smaguma pakāpe – tie tūlītējie vai aizkavētie scenāriji, kas var izraisīt vai veicināt drošuma incidentus, ar incidentu saprotot jebkādu ar lidaparāta ekspluatāciju saistītu notikumu, kurš nav nelaimes gadījums un kurš ietekmē vai varētu ietekmēt ekspluatācijas drošumu;
* zema smaguma pakāpe – tie tūlītējie vai aizkavētie scenāriji, kas var radīt vai veicināt nelielu ietekmi uz drošumu.

*EUROCAE* dokumenta ED-201A B papildinājumā par produktiem, *ATM* sistēmām un gaisa telpu ir sniegti piemēri attiecībā uz augstu, vidēju un zemu smaguma pakāpi.

Ja organizācija nevar noteikt ietekmi uz drošumu, novērtējumā jānosaka pieņēmumi no riska dalīšanas informācijas, kura iegūta saskarnēs ar citām organizācijām funkcionālajā ķēdē, lai tādējādi noteiktu ietekmi uz drošumu.

Dažus no šiem pieņēmumiem var nodrošināt līdz ar produktu sertifikāciju – ja aktīviem tiek piemērota produkta sertifikācija, ko paredz citi aviācijas noteikumi, kuros ir apspriesta produkta informācijas drošība, tad organizācija, kas veic riska novērtējumu, var uzskatīt, ka produkta sertifikācijas tvērums jau ir nosegts. Šādai kārtībai ir jābūt pieļaujamai ar nosacījumu, ka šis sertifikāts ir derīgs un organizācija īsteno pamatiekārtu ražotāju sniegtos norādījumus par sertifikācijas derīguma saglabāšanu.

Papildu informācija ir sniegta arī Regulā (ES) 2015/1018 par obligātu ziņošanu par atgadījumiem civilajā aviācijā. Citi piemēri par ietekmes smaguma pakāpes klasifikāciju aviācijas jomās ir sniegti *EUROCAE* dokumenta ED-201A B papildinājuma B-5., B-6. un B-7. tabulā.

**Riska pieņemšanas kritēriji**

Riska pieņemšanas kritērijiem ir būtiska nozīme, un tie ir jāizstrādā, jāprecizē un jādokumentē. Ar kritērijiem var noteikt vairākas robežvērtības ar vēlamo riska līmeni, vienlaikus ļaujot atbildīgajam vadītājam vai deleģētai(-ām) personai(-ām) noteiktos apstākļos un atbilstoši noteiktiem nosacījumiem pieņemt riskus, kuri pārsniedz šo līmeni.

Lai atvieglotu riska novērtējumu savstarpējo salīdzināmību starp saskarstruktūrām, organizācijai riski jāklasificē šādās kategorijās:

* nepieņemams risks;
* nosacīti pieņemams risks;
* pieņemams risks.

Attiecībā uz risku nosacītu pieņemšanu, pieņemšanas kritērijos jāņem vērā paredzamais riska pastāvēšanas laiks (īslaicīga vai īstermiņa darbība vai pakļautība riskam), vai arī tajos var ietvert prasības attiecībā uz apņemšanos turpināt risku mazināšanu pieņemamā līmenī noteiktā periodā un parādīt to, kā risks tiks pārvaldīts laika gaitā, izmantojot organizācijas riska pārvaldības procesus.

Turklāt riski ir jāpieņem nosacīti tikai tad, ja organizācija pierāda tādas vispusīgas riska pārvaldības struktūras pastāvēšanu, kas ietver riska novērtēšanu, riska risināšanu un riska uzraudzības procesus attiecībā uz darbību. Riska pārvaldībā jāņem vērā apdraudējuma iespējamības, ievainojamības, pašreizējo kontroles pasākumu, ārējās atkarības un ietekmes uz drošumu mainīgums un saskanība. Tas parasti tiek panākts, ja organizācija sasniedz augstāku gatavības pakāpi, kas atbilst informācijas drošības riska pārvaldības funkcionalitātei un atkārtojamībai – skat. GM1 par IS.I.OR.260. punkta a) apakšpunktu.

Turpmāk 1. attēlā parādīta riska pieņemšanas tabula, kuras pamatā ir iepriekš minētās kategorijas, ko saskarorganizācijas var izmantot savstarpējai salīdzināmībai.

|  |  |  |  |
| --- | --- | --- | --- |
| *ICAO* 13. pielikums > | Neliela ietekme | Incidents | Nelaimes gadījums |
| Apdraudējuma scenārijs – īstenošanās iespējamība | **Zema ietekme uz drošumu** | **Vidēja ietekme uz drošumu** | **Augsta ietekme uz drošumu** |
| **Augsta** | Nosacīti pieņemams | **Nepieņemams** | **Nepieņemams** |
| **Vidēja** | Pieņemams | Nosacīti pieņemams | **Nepieņemams** |
| **Zema** | Pieņemams | Pieņemams | Nosacīti pieņemams\* |

**1. attēls. Riska pieņemšanas tabulas piemērs salīdzināšanai**

\* Apdraudējuma scenārija īstenošanās iespējamība tiek savlaicīgi atkārtoti novērtēta (skat. IS.I.OR.205. punkta d) apakšpunktu) un uzraudzīta, lai nodrošinātu, ka tā saglabājas zema un ka riska īstenošanās gadījumā tas tiek savlaicīgi atklāts un risināts.

Visaptveroša riska pārvaldības struktūra parasti ietver šādus aspektus un procesus:

* atkārtojams un reproducējams riska novērtējums. Ja riska faktori tiek uzskatīti par diezgan neskaidriem un ietilpstošiem plašā vērtību diapazonā vai par nepietiekami precīziem, veic turpmākus riska novērtējuma atkārtojumus, ietverot papildus apkopotu vai detalizētu informāciju un padziļinātāku novērtējumu, lai samazinātu nenoteiktību un palielinātu precizitāti;
* rūpīgs to risku izvērtējums, kas ierosināti kā nosacīti pieņemami, kuru veic atbildīgais vadītājs vai deleģēta(-as) persona(-as), kura(-as) var noteikt papildu nosacījumus riska ierobežošanai, tostarp riska risināšanas pasākumu un tā īstenošanas grafiku;
* galveno riska rādītāju stingra uzraudzība, kas ietver noteiktu, ticamu iespējami mainīga riska īstenošanās atklāšanu;
* ir ieviesta sistēma reaģēšanai uz incidentiem ar atbildes pasākumiem, kurus aktivizē atklāšanas mehānismi, lai nekavējoties ierobežotu sekas, jo īpaši attiecībā uz riska scenārijiem ar augstu smaguma pakāpi.

Piezīme. Kā sīkāk izklāstīts NIST SP-800 Rev.1, atkārtojamība ir spēja atkārtot novērtējumu tādā veidā, kas ir saskanīgs ar iepriekšējiem novērtējumiem un līdz ar to ir salīdzināms ar tiem, ļaujot organizācijai noteikt tendences. Tāpēc riska novērtēšanas procesu var klasificēt kā “atkārtojamu”, ja līdzīgos apstākļos struktūra vai persona iegūst saskanīgus rezultātus.

Kā sīkāk izklāstīts NIST SP-800 Rev.1, reproducējamība ir dažādu ekspertu spēja iegūt vienādus rezultātus no vieniem un tiem pašiem datiem. Līdz ar to riska novērtēšanas procesu var klasificēt kā “reproducējamu”, ja cita struktūra vai persona, izmantojot tos pašus ievaddatus, pieņēmumus, informācijas drošības kontekstu un apdraudējuma vidi, var atkārtot tās pašas darbības un nonākt pie tiem pašiem secinājumiem.

**Apdraudējuma scenārija noteikšana**

Apdraudējuma scenārijs ir viens no iespējamajiem veidiem, kā apdraudējums varētu īstenoties. Parasti apdraudējuma scenārijā ir aprakstīts iespējamais uzbrukums, kas ir vērsts pret vienu vai vairākām aktīvu un arī procesu ievainojamībām.

Apdraudējuma scenārija noteikšanas mērķis saskaņā ar šo regulu ir izstrādāt sarakstu ar scenārijiem, kas var radīt tādu informācijas drošības apdraudējumu, kurš ietekmē aviācijas drošumu.

Apdraudējuma scenāriju kopumā raksturo šādi elementi:

* uzbrukuma informācijas drošībai apdraudējuma avots;
* uzbrukuma vektors un ceļš caur organizāciju līdz aktīvam;
* informācijas drošības kontroles pasākumi, kas mazinātu uzbrukuma ietekmi;
* uzbrukuma sekas, tostarp ietekmētie drošuma aspekti.

Norādījumi par apdraudējuma scenārija noteikšanu ir sniegti *EUROCAE* dokumenta ED-202A 3.4. nodaļā. Tas nav vienīgais norādījumu avots, un organizācija var izmantot citus norādījumus, kas ir piemērotāki tās vajadzībām.

**Papildu metodes atbilstošu apdraudējuma scenāriju noteikšanai**

Veicot šo analīzi, visa procesa laikā ir jāsaskaņo informācijas drošības un drošuma aspekti, lai nodrošinātu savstarpēju izpratni par piemērotajiem apdraudējuma novēršanas un mazināšanas pasākumiem. Turpmāk 2. attēlā mijiedarbība starp informācijas drošību un aviācijas drošumu ir attēlota, izmantojot tauriņveida diagrammu, kurā izceltas saites starp riska kontroles pasākumiem un pamatā esošo pārvaldības sistēmu.

****

**2. attēls. Mijiedarbība starp informācijas drošības un aviācijas drošuma riska pārvaldības jomām**

Piezīme. Preventīva barjera jeb pasākums ir preventīva darbība vai kontroles pasākums, ko īsteno, lai mazinātu riska, bīstamības vai apdraudējuma īstenošanās iespējamību, savukārt mazinošs pasākums ir darbība vai kontroles pasākums, kura mērķis ir samazināt nevēlama notikuma smaguma pakāpi vai ietekmi tā īstenošanās gadījumā.

**Apdraudējuma scenāriju piemēri**

Apdraudējumu katalogi var sniegt norādījumus un elementus tādu apdraudējuma scenāriju izstrādei, kas attiecas uz organizāciju. Dokumenta ARINC 811 – Att. 3 – 3-7. un 3-8. tabulā sniegtas norādes par apdraudējuma katalogu piemēriem un citu apdraudējuma katalogu piemēriem, ko sniegušas ES iestādes, piemēram, par *ENISA* veidoto apdraudējuma taksonomiju. Tomēr tas nav pilnīgs piemēru saraksts, tāpēc apdraudējuma scenāriju noteikšanā jāizmanto ne tikai šie piemēri. Turklāt, lai nodrošinātu nepieciešamos ievaddatus riska novērtēšanas procesam, jāizmanto citi atbilstoši resursi, kas ietver informāciju par informācijas drošības apdraudējumu un informācijas drošības apdraudējuma ainu.

Apdraudējuma scenāriju piemēri ir apkopoti I papildinājumā.

## AMC1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu

Nosakot atbilstību IS.I.OR.205. punkta d) apakšpunktā minētajiem mērķiem, organizācijai ir jāņem vērā šādi kritēriji:

a) riska novērtējums, kas veikts saskaņā ar IS.I.OR.205. punkta a), b) un c) apakšpunktu, ir regulāri jāpārskata, lai noteiktu un ņemtu vērā attiecīgās izmaiņas. Iespējamo izmaiņu izvērtēšanas periodiskums jānosaka organizācijai, kas veic novērtējumu, ņemot vērā riska novērtējuma tvērumā ietilpstošo aktīvu kritiskumu, riska novērtējuma tvērumā ietilpstošo aktīvu atlikušā riska līmeņus un jebkādas līgumiskas vai reglamentējošas prasības. Ja kritiskuma pakāpe vai riska līmenis ir augstāks, pārskatīšana būs jāveic biežāk;

b) organizācijai ir jādokumentē riska novērtējuma pārskatīšanas periodiskums un jāsniedz pamatojums, jānorāda apstiprināšanas datums un informācija par riska īpašnieku.

## GM1 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu

Kritēriji, kas jāņem vērā, nosakot riska novērtējuma pārskatīšanas biežumu, var būt riska līmenis, kā arī attiecīgo aktīvu kritiskums un sarežģītība. Riska novērtējuma pārskatīšanas mērķis ir ierosināt risku, to iespējamības un ietekmes atkārtotu novērtēšanu būtisku izmaiņu gadījumā. Viens no iespējamajiem veidiem ir daudzpakāpju pieeja riska novērtēšanai, izmaiņu noteikšanai izmantojot augstāka līmeņa riska novērtējumu. Izmantojot augstāka līmeņa riska novērtējumu, var būt iespējams noteikt detalizētus riskus, kas jāizvērtē nākamajā posmā. Riska novērtējumi ir regulāri jāpārskata, lai:

a) varētu pastāvīgi uzlabot riska novērtējuma kvalitāti;

b) nodrošinātu riska kontroles pasākumu un mazinošo pasākumu efektivitāti un rezultativitāti gan to izstrādē, gan darbībā;

c) pārskatītu riska risināšanas plānus un pasākumus;

d) noteiktu jebkādas organizatoriskas izmaiņas, kuru dēļ var būt jāpārskata prioritātes un risku risināšana;

e) nodrošinātu pilnīgu pārskatu par risku kopainu un

f) noteiktu visus iespējamos riskus.

Riska novērtējuma pārskatīšanā attiecīgā gadījumā jāiesaista riska īpašnieki, projektu grupas un citas ieinteresētās personas. Riska novērtējuma pārskatīšanas pierādījumi ir jādokumentē, un tajos ir jāietver:

* pierādījumi par to, ka izraudzītais riska īpašnieks ir apstiprinājis pārskatīšanu, un
* iemesls vai pamatojums riska īpašnieka veiktajam pārskata apstiprinājumam.

Cita starpā šādi pierādījumi var ietvert:

* ziņojumus, kas veido dokumentāciju to informācijas drošības risku izsekošanai, kuri var ietekmēt organizāciju;
* informācijas drošības riska novērtējuma dokumentāciju;
* izrakstus no darbības vai drošības risku reģistra.

Organizācijai riska novērtējuma pārskatīšanas periodiskums ir jādokumentē arī informācijas drošības rokasgrāmatās, procesos vai procedūrās, un tam ir jābūt saskanīgam ar plašākiem izmaiņu pārvaldības pasākumiem un informācijas drošības pārvaldības pārskatiem. Papildu norādījumi par riska novērtējuma pārskatīšanas kritērijiem un biežumu ir sniegti *EUROCAE* dokumenta ED-201A 4. nodaļā un arī *EUROCAE* dokumenta ED-205A 3.2. nodaļā (attiecībā uz *ATMS*/*ANS*).

## GM2 par IS.I.OR.205. punkta “Informācijas drošības riska novērtējums” d) apakšpunktu

Turpmāk sniegti piemēri izmaiņām, kas ir jāidentificē riska novērtējuma pārskatīšanas laikā, jo to dēļ var būt nepieciešama riska novērtējuma atjaunināšana:

a) ir notikušas izmaiņas elementos, uz kuriem attiecas informācijas drošības riski, kā noteikts IS.I.OR.205. punkta a) apakšpunktā; izmaiņas elementos ietver:

* atsevišķu elementu riska novērtējuma tvēruma papildināšanu vai samazināšanu;
* izmaiņas riska novērtējuma tvērumā ietilpstošo elementu uzbūvē vai konfigurācijā, kas var mainīt riska novērtējuma rezultātus, vai
* izmaiņas vērtībās, kas varētu izraisīt izmaiņas riska novērtējuma tvērumā ietilpstošo elementu ietekmes līmeņos;

b) ir notikušas izmaiņas saskarnēs starp organizāciju un citām organizācijām, ar kurām organizācijai ir kopīgi informācijas drošības riski vai uz kurām tā paļaujas, lai mazinātu informācijas drošības riskus (piemēram, piegādes ķēdes, pakalpojumu sniedzēji, mākoņpakalpojumu sniedzēji un klienti), kā noteikts IS.I.OR.205. punkta b) apakšpunktā, vai starp sistēmu, kas ietilpst riska novērtējuma tvērumā, un citām savienotām sistēmām, vai ir mainījušies riski, par kuriem organizācijai paziņojušas citas organizācijas, kā norādīts IS.I.OR.205. punkta b) apakšpunktā, vai citu sistēmu īpašnieki vai pārvaldnieki, tostarp:

* jaunu saskarņu izveide;
* pašreizējo saskarņu likvidēšana;
* izmaiņas pašreizējās saskarnēs, kas varētu mainīt riska novērtējuma rezultātus.

Piezīme. Daži organizatoriski vai sistēmu savienojumi var būt izveidoti ar organizācijām, kas neietilpst šīs regulas darbības jomā, kura noteikta 2. pantā, un tāpēc uz tām neattiecas *IS* daļas prasības. Šādā gadījumā šīs organizācijas ir jāinformē par to pienākumu ziņot par iepriekš minētajām izmaiņām, katrā atsevišķā gadījumā un atbilstoši vajadzībai ar iesaistītajām organizācijām noslēdzot līgumiskas vienošanās un piemērojot ziņošanas prasības;

c) ir notikušas izmaiņas informācijā vai zināšanās, ko izmanto risku identificēšanai, analīzei un klasificēšanai, tostarp:

* apdraudējumu un to vērtību izmaiņas vai jaunu, iepriekš nenovērtētu apdraudējumu pievienošana;
* izmaiņas ievainojamībās vai jaunu, iepriekš nenovērtētu ievainojamību pievienošana;
* novērtēto apdraudējumu vai ievainojamību ietekmes vai seku izmaiņas;
* izmaiņas risku apkopojumā, kas var radīt nepieņemamus risku līmeņus;
* izmaiņas vai uzlabojumi riska pārvaldības procesā, riska novērtēšanas pieejā un saistītajos pasākumos;
* izmaiņas vai uzlabojumi risku risināšanā;
* izmaiņas kritērijos, ko izmanto, lai noteiktu risku pieņemšanu un risināšanu;

d) ir gūtas atziņas no informācijas drošības incidentu analīzes, tostarp:

* gūta izpratne par to, kāpēc un kā incidenti ir notikuši, un
* pārskatīti visi incidentu veidi, tostarp tie, kurus izraisījuši ārēji faktori, tehniski iemesli, cilvēka kļūdas (netīša rīcība). Attiecībā uz tīšu cilvēka rīcību var nošķirt ļaunprātīgas un nekaitīgas darbības.

## AMC1 par IS.I.OR.205. punkta e) apakšpunktu “Informācijas drošības riska novērtējums”

**DROŠĪBAS ATBALSTA NOVĒRTĒJUMS**

Pakalpojumu sniedzējiem, kas nav *ATS* nodrošinātāji, jāveic drošības atbalsta novērtējums, kā aprakstīts Regulā (ES) 2017/373, lai novērtētu informācijas drošības risku attiecībā uz to aktīviem saistībā ar pakalpojuma specifikāciju, piemēram, integritāti un pieejamību, un lai noteiktu nenovērsto risku.

Pakalpojumu sniedzējam, kas nav *ATS* nodrošinātājs, atbilstošā veidā būtu jāsniedz *ATS* nodrošinātājam informācija par nenovērsto risku un ietekmi uz pakalpojumiem, ko tas sniedz šim *ATS* nodrošinātājam.

Nenovērstais risks būtu jāizmanto, lai novērtētu iespējamo ietekmi uz pakalpojumiem un produktiem, ko pakalpojumu sniedzējs, kas nav *ATS* nodrošinātājs, piedāvā *ATS* nodrošinātājam.

*ATS* nodrošinātājs var izmantot šo informāciju kā ievaddatus savam drošības riska novērtējumam un, kas ir vēl svarīgāk, lai novērtētu šo nenovērsto risku iespējamo ietekmi uz drošību.

## GM1 par IS.I.OR.205. punkta e) apakšpunktu “Informācijas drošības riska novērtējums”

**DROŠĪBAS ATBALSTA NOVĒRTĒJUMS**

Turpmāk 1. tabulā ir norādīti pakalpojumu sniedzēji, kas nav *ATS* nodrošinātāji un kam jānodrošina atbilstība Regulas (ES) 2017/373 III pielikuma C apakšiedaļas prasībām. Tās ir organizācijas, kurām ir jāveic drošības atbalsta novērtējums, lai sniegtu nepieciešamo informāciju *ATS* nodrošinātājiem.

Pakalpojumu sniedzēji, kas nav *ATS* nodrošinātāji, un *ATS* nodrošinātāji var apmainīties ar informāciju par ietekmi uz produktiem un pakalpojumiem, izmantojot saskaņotus līdzekļus, piemēram, pakalpojumu līmeņa vienošanos, ārēju vienošanos (saskaņā ar *EUROCAE* dokumentu ED-201A) utt.

Informācijai, ar kuru apmainās, būtu jāļauj *ATS* nodrošinātājiem veikt precīzu nenovērstā riska novērtējumu attiecībā uz to pakalpojumiem. Piemēram, ja pakalpojumu sniedzēji, kas nav *ATS* nodrošinātāji, ir noteikuši risku, kas varētu ietekmēt *ATS* nodrošinātājam sniegto datu pieejamību, ietekme uz pieejamību būtu jāapraksta tā, lai *ATS* nodrošinātājs varētu novērtēt, vai izrietošais datu pārsūtīšanas gaidīšanas laiks vai kavējums varētu ietekmēt drošību. Tas ir būtiski, jo tikai *ATS* nodrošinātājs, veicot novērtējumu, var pieņemt vai noraidīt nenovērsto risku.

**1. tabula. Pakalpojumu sniedzēji, kas nav *ATS* nodrošinātāji, kuriem jānodrošina atbilstība Regulas (ES) 2017/373 III pielikuma C apakšiedaļas prasībām**

****

|  |  |
| --- | --- |
| **Angļu val.** | **Latviešu val.** |
| Annex IIII (Part-ATM/ANS.OR) | IIII pielikums (ATM/ANS.OR daļa) |
| Subpart A | A apakšiedaļa |
| Subpart B | B apakšiedaļa |
| Subpart C | C apakšiedaļa |
| Subpart D | D apakšiedaļa |
| Annex IV (Part- ATS) | IV pielikums (*ATS* daļa) |
| Annex V (Part- MET) | V pielikums (*MET* daļa) |
| Annex VI (Part- AIS) | VI pielikums (*AIS* daļa) |
| Annex VII (Part- DAT) | VII pielikums (*DAT* daļa) |
| Annex VIII (Part- CNS) | VIII pielikums (*CNS* daļa) |
| Annex IX (Part- ATFM) | IX pielikums (*ATFM* daļa) |
| Annex X (Part- ASM) | X pielikums (*ASM* daļa) |
| Annex XI (Part- FPD) | XI pielikums (*FPD* daļa) |
| Annex XII (Part- NM) | XII pielikums (*NM* daļa) |
| Air traffic services providers | Gaisa satiksmes pakalpojumu sniedzēji |
| Metereological services providers | Metereoloģisko pakalpojumu sniedzēji |
| Aeronautical information services providers | Aeronavigācijas informācijas pakalpojumu sniedzēji |
| Data services providers | Datu pakalpojumu sniedzēji |
| Communication, navigation and surveillance service providers | Saziņas, navigācijas un uzraudzības pakalpojumu sniedzēji |
| Air traffic flow management service providers | Gaisa satiksmes plūsmas vadības pakalpojumu sniedzēji |
| Airspace management service providers | Gaisa telpas pārvaldības pakalpojumu sniedzēji |
| Flight procedure design services providers | Lidojuma procedūru izstrādes pakalpojumu sniedzēji |
| Network Manager | Tīkla pārvaldnieks |

## GM1 par IS.I.OR.210. punktu “Informācijas drošības riska risināšana”

Attiecībā uz nepieņemamiem riskiem, kas ir noteikti saskaņā ar IS.I.OR.205. punktu, jāpiemēro riska risināšanas process, kura rezultātā var būt jāievieš informācijas drošības pasākumi, ko bieži dēvē par informācijas drošības kontroles pasākumiem.

Attiecībā uz katru noteikto risku organizācijai jānosaka konkrēti riska risināšanas pasākumi, paņēmieni vai resursi, kas tiks izmantoti katra aktīva dzīves ciklā, lai:

* pārvaldītu riska mazināšanu;
* uzraudzītu un uzturētu katru aktīvu;
* atjauninātu un izpildītu konfigurāciju pārvaldības pasākumus;
* pārvaldītu piegādes ķēdi;
* pārvaldītu nolīgtos pakalpojumus vai pakalpojumu sniedzēju.

Riska risināšanas pasākumu pārskatā jāiekļauj ar iekārtām, procedūrām un personālu saistītie dzīves cikla apsvērumi.

Riska risināšanas plānā, kas sagatavots riska pārvaldības procesā, jāietver risku prioritāšu noteikšana, atbilstoša informācija par riska risināšanas mērķiem un līdzekļiem, kuri jāizmanto, lai sasniegtu pieņemamu riska līmeni, kā arī jānorāda saskaņoti termiņi, kuros atbildīgajam personālam ir jāīsteno riska risināšanas pasākumi. Par riska risināšanas pasākuma īstenošanas termiņiem jāvienojas personālam, kas atbild par īstenošanu, un tie ir jāpaziņo atbildīgajam vadītājam vai deleģētajai(-as) personai(-as), kuri tos apstiprina.

Attiecībā uz riskiem, kas var radīt nedrošus apstākļus, riska risināšanas plānā ir jādokumentē ikviens turpmākais īstenošanas kavējums un jānorāda tā cēlonis, iemesls vai nepieciešamība. Ja riska īstenošanās radītu nedrošu stāvokli, atjauninātā riska risināšana ir jādara zināma kompetentajai iestādei. Kavēšanās ir jāapstiprina arī organizācijas atbildīgajam vadītājam vai deleģētajai(-ajām) personai(-ām). Šī persona var izvirzīt nosacījumu, ka piekrišana tiks sniegta tikai tad, kad būs ieviesti vai pieejami kompensējoši kontroles pasākumi vai atbildes pasākumi, lai uzraudzītu, savlaicīgi atklātu un savlaicīgi reaģētu uz risināmo risku. Lai savlaicīgi reaģētu, var informēt ātrās reaģēšanas vienību, lai nodrošinātu tās gatavību.

Riska risināšanas plānu var izmantot kā līdzekli saziņai ar kompetento iestādi, lai parādītu, ka nepieņemamie riski tiek efektīvi risināti. Tāpat šo plānu var izmantot, lai saskarorganizācijām darītu zināmu, kā tiek kontrolēti kopīgie riski.

Saskaņā ar IS.I.OR.205. punkta d) apakšpunktu riska novērtējums ir jāpārskata regulāri vai noteiktos gadījumos, un šāda pārskatīšana ietver atbilstoši IS.I.OR.210. punkta a) apakšpunktam izstrādāto riska risināšanas pasākumu pārskatīšanu, lai noteiktu, vai tie joprojām ir efektīvi vai tiem nepieciešami pielāgojumi.

Turklāt gadījumā, ja mijiedarbībā starp saskarstruktūrām var rasties kopīgs informācijas drošības risks, organizācijai jāapsver arī iespējamā ietekme uz riska risināšanas pasākumu rezultativitāti (skat. IS.I.OR.235. punktu un saistītos *AMC*).

## AMC1 par IS.I.OR.210. punkta “Informācijas drošības riska risināšana” a) apakšpunktu

a) Riska risināšanas procesā jāsasniedz vismaz viens no IS.I.OR.210. punkta a) apakšpunktā minētajiem mērķiem.

b) Nosakot atbilstību IS.I.OR.210. punkta a) apakšpunkta 1) daļā un IS.I.OR.210. punkta a) apakšpunkta 2) daļā noteiktajiem mērķiem, organizācijai jāņem vērā, ka:

1) pasākumi, kas izstrādāti atbilstoši šiem punktiem, jāīsteno saskaņā ar riska risināšanas plānu ar noteiktām, uz risku balstītām prioritātēm, mērķiem un saskaņotiem termiņiem un īpašniekiem;

2) dzīves cikla apsvērumiem jābūt noteiktiem un saistītiem, lai nodrošinātu informācijas drošības pasākumu, tostarp datu apmaiņas ar citām struktūrām, pastāvīgu rezultativitāti;

3) tai ir jāpārskata un jāatjaunina riska novērtējums saskaņā ar IS.I.OR.205. punkta d) apakšpunktu, lai novērtētu, vai atbilstoši šiem punktiem izstrādātie pasākumi rada jaunus nepieņemamus riskus vai maina pašreizējos riskus tā, ka tie kļūst nepieņemami.

c) Riska risināšana ir jādokumentē un jāreģistrē, piemēram, risku reģistrā, pat ja risks ir novērsts.

## AMC1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

Organizācijām kā avots jāizmanto incidenti, kas konstatēti to pasākumu laikā, kuri veikti, lai pierādītu atbilstību IS.I.OR.220. punkta a) apakšpunktam. Organizācijām jābūt mehānismam, lai apkopotu personāla un ārpus uzņēmuma esošo avotu, tostarp piegādātāju, partneru, klientu, atklātā pirmkoda programmatūras un informācijas drošības pētnieku sniegtos paziņojumus par notikumiem. Mehānismam, kas paredzēts informācijas vākšanai, kuru veic personāls un ārējie avoti, jābūt viegli pieejamam un paziņojamam.

Organizācijai jāapkopo ar atklāšanas līdzekļiem iegūtā un iekšējai analīzei paredzētā informācija par visiem notikumiem. Katrs notikums ir jāanalizē, lai noteiktu, vai par to ir jāziņo un, ja ir, kāda ir bijusi iespējamā vai faktiskā ietekme uz aviācijas drošumu. Informācijas drošības notikumi jāaplūko kopā ar citiem notikumiem, lai nodrošinātu korelāciju ar mērķi noteikt incidentus vai ievainojamības, kas var ietekmēt aviācijas drošumu.

Organizācijai jāizskata riska novērtējuma rezultāti un to jauno ievainojamību izmantošanas iespējas, kas konstatētas atklāšanas pasākumos, kuri veikti atbilstoši IS.I.OR.220. punkta a) apakšpunktā noteiktajiem pasākumiem.

Organizācijai jānosaka visas iekšējās ieinteresētās personas, kam nepieciešams paziņojums par konkrētu incidentu vai ievainojamību, un jānodrošina, ka šīs ieinteresētās personas saņem visu nepieciešamo informāciju par incidentu vai ievainojamību, lai efektīvi un savlaicīgi rīkotos noteiktajos atklāšanas un reaģēšanas periodos.

## GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

**SAISTĪBA STARP IEKŠĒJO UN ĀRĒJO ZIŅOŠANU**

Organizācijām jāapkopo un iekšēji jāziņo informācija par incidentiem un ievainojamībām, lai aptvertu visus šīs regulas darbības jomā ietilpstošos jautājumus. Lai nodrošinātu ziņošanas sistēmas pilnīgumu un efektivitāti, ir nepieciešama gan iekšējā, gan ārējā ziņošana. Iekšējie ziņojumi jāizvērtē savlaicīgi, un, ja iespējamā ietekme uz drošību rada nedrošu stāvokli, organizācijām jāsāk ziņot par šiem iekšējiem ziņojumiem atbilstoši IS.I.OR.230. punktam.

## GM2 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

**INFORMĀCIJAS DROŠĪBAS NOTIKUMU APKOPOŠANAS UN IZVĒRTĒŠANAS ORGANIZĒŠANA**

Lielās organizācijās ir izplatīta prakse informācijas drošības darbības centralizēt drošības darbību centrā (*SOC*) un izmantot informācijas drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmu. *SIEM* sistēmā apkopo visus notikumus no avotiem, piemēram, no žurnalēšanas datnēm, kopējā datu bāzē, un tā ļauj analizētājiem un reaģētājiem vienotā *SOC* pārbaudīt šos notikumus un reaģēt uz tiem. Organizācijas var izvēlēties izmantot *SOC* attiecībā uz notikumiem, kuri ir saistīti ar *IS* daļu, atsevišķi vai kopā ar notikumiem, uz kuriem neattiecas *IS* daļa, bet kuri interesē organizāciju, piemēram, ar notikumiem, kas ir saistīti ar uzņēmējdarbības interesēm. Notikumus var automātiski apkopot, savstarpēji saistīt un analizēt, lai atklātu normai neatbilstošu rīcību, kas izraisa informācijas drošības incidentus.

Organizācijām, kam nav *SOC* iespēju un kas neizmanto *SIEM* sistēmu, ir jāapsver, kā izveidot procesus, lai nodrošinātu nepieciešamās apkopošanas un izvērtēšanas spējas, kā arī atklāšanas un reaģēšanas laiku.

## GM3 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

**BŪTISKĀ INFORMĀCIJA PAR INCIDENTIEM UN IEVAINOJAMĪBĀM**

Izpratne par informācijas drošības incidentu un ievainojamību, kuri ir saistīti ar *IS* daļu, cēloņiem un veicinošajiem faktoriem ļauj gūt pieredzi un pielāgot procesus un aktīvu izstrādi. Tomēr cēloņus un veicinošos faktorus ne vienmēr ir iespējams izprast, vai arī šāda izpratne var nepalīdzēt pastāvīgi uzlabot aviācijas drošumu. Ja ievainojamību rada aktīvi, kas izstrādāti tikai vai galvenokārt aviācijai, ir sagaidāms, ka būs iespējams veikt nepieciešamo izpēti par galvenajiem cēloņiem. Informācija par šiem galvenajiem cēloņiem palīdzēs organizācijai(-ām) uzlabot procesus un aktīvu izstrādi, lai novērstu ievainojamību un nodrošinātu, ka šādas ievainojamības netiek ieviestas citos aktīvos. Izpratne par ievainojamību galvenajiem cēloņiem ļauj arī aviācijas kopienai mācīties un tādējādi turpmāk novērst līdzīgas ievainojamības.

## GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” c) apakšpunktu

Ja šī regula attiecas arī uz nolīgtajām organizācijām, informācijas apmaiņai un ziņošanai jābūt ietvertai kopīgo risku pārvaldībā un nodrošinātai, noslēdzot ārēju vienošanos starp organizācijām. Norādījumi par ārējo vienošanos izstrādi ir sniegti *EUROCAE* dokumenta ED-201A 4.4. nodaļā “Ārējās vienošanās”.

Kopumā un visos pārējos gadījumos jebkurā pakalpojumu līgumā ir jāiekļauj standarta noteikumi par nolīgtās organizācijas pienākumu:

* noteiktā laikā ziņot par informācijas drošības incidentiem, kuri var ietekmēt līgumslēdzēju organizāciju. Par incidentiem un ievainojamībām, kas varētu radīt nedrošus apstākļus, jāziņo iespējami drīz un tā, lai varētu izpildīt ārējās ziņošanas pienākumu atbilstoši IS.I.OR.230. punktam;
* izraudzīties kontaktpunktu incidentu pārvaldībai un iespējamai krīžu pārvaldībai.

Dažos gadījumos nolīgtās organizācijas, piemēram, pakalpojumu sniedzēji ar dalītiem resursiem, var nespēt piedāvāt *ad hoc* ziņošanu. Šādos gadījumos iekšējās ziņošanas prasību var izpildīt ar citiem līdzekļiem, kas atbilst šā noteikuma mērķim. Piemēram, nolīgtās organizācijas var iesniegt atjauninātu to ievainojamību sarakstu, kas ietekmē sistēmas, uz kurām attiecas nolīgtie pakalpojumi. Līgumslēdzējai organizācijai šis saraksts jāuzrauga iekšējās ziņošanas par informācijas drošības notikumiem ietvaros.

## GM1 par IS.I.OR.215. punkta “Sistēma iekšējai ziņošanai par informācijas drošību” d) apakšpunktu

Sadarbību, kura paredzēta IS.I.OR.215. punkta d) apakšpunktā, var stiprināt, apmainoties ar elementiem no incidentu dokumentācijas, kas var noderēt citu organizāciju informācijas drošības pasākumiem. Ja organizācijām ir līgumsaistības, šis līgums var ietvert arī apņemšanos sadarboties. Organizācijas var apsvērt iespēju izstrādāt oficiālas vienošanās (piemēram, saprašanās memorandu), kurās izklāstītas funkcijas un pienākumi attiecībā uz sadarbību informācijas drošības jomā, piemēram, pārvaldības sanāksmes, kopīgi attīstības pasākumi un kompromitējuma rādītāju (*IoC*) apmaiņa reālajā laikā.

Turklāt apņemšanos sadarboties var panākt arī ar organizācijas aktīvu līdzdalību informācijas drošības apmaiņas iniciatīvās, piemēram, *ISAC* iniciatīvā(-ās). Turklāt savas informētības uzlabošanas nolūkā organizācijas var arī piekrist saņemt ievainojamības un apdraudējuma brīdinājumus, piemēram, *CERT* izplatītos brīdinājumus.

## GM1 par IS.I.OR.220. punktu “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana”

Neskarot “informācijas drošības notikuma” definīciju Regulas (ES) 2023/203 3. pantā, notikumi, kas norāda uz nepieņemamu risku iespējamu īstenošanos, ietver gan atgadījumus (t. i., jebko, kas rada vai var radīt kaitējumu), gan ievainojamību atklāšanu. Informācijas drošības riski faktiski ir saistīti ar iespējamību, ka apdraudējums izmantos ievainojamības, tāpēc izmantojamas ievainojamības atklāšana ir informācijas drošības notikums.

Ņemot to vērā, saistībā ar šo regulu:

* IS.I.OR.220. punkta a) apakšpunktā noteiktie atklāšanas pasākumi ietver ievainojamību atklāšanu;
* IS.I.OR.220. punkta b) apakšpunktā noteiktie reaģēšanas pasākumi ietver ievainojamību pārvaldību.

## AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” a) apakšpunktu

**ATKLĀŠANA**

Izpildot IS.I.OR.220. punkta a) apakšpunktā noteikto prasību, organizācijai jānosaka un jāīsteno stratēģija, lai atklātu informācijas drošības incidentus, kas var ietekmēt drošumu.

Tas jādara tā, lai nodrošinātu, ka ar atklāšanas stratēģiju var aptvert vismaz visus zināmos informācijas drošības apdraudējumus to aktīviem, kas var kļūt par drošuma apdraudējumu ar nepieņemami smagām sekām.

**ATKLĀŠANAS STRATĒĢIJA**

Lai noteiktu notikuma atklāšanas tvērumu, organizācijai jāveic šādas darbības:

a) jānosaka apdraudējuma scenāriju saraksts no riskiem, kas noteikti atbilstoši IS.I.OR.205. punktam;

b) jānosaka vismaz tie aktīvi, kuri to apdraudējuma gadījumā veicinātu tāda(-u) scenārija(-u) īstenošanos, kas varētu kļūt par nedrošu stāvokli. Lai noteiktu šos aktīvus, ir jāņem vērā arī IS.I.OR.210. punktā paredzētie pasākumi.

Piezīme. Aktīva nozīme apdraudējuma scenārijā un nedroša stāvokļa īstenošanās jānovērtē, ņemot vērā arī visu funkcionālo ķēdi. Dažos gadījumos aktīvs var atrasties funkcionālās ķēdes beigās, un, ja tas tiek apdraudēts, ietekme uz drošumu ir tieša un var būt tūlītēja; savukārt, ja aktīvs atrodas tālu no funkcionālās ķēdes beigām un tas tiek apdraudēts, ietekmei ir jāizplatās un tā var būt aizkavēta.

## GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” a) apakšpunktu

**ATKLĀŠANAS STRATĒĢIJA**

Izstrādājot atklāšanas stratēģiju, organizācijai attiecībā uz vienumiem, kas ietilpst notikumu atklāšanas tvērumā, ir jānosaka apstākļi, kuros ir jāierosina process, kam, piemēram, būtu nepieciešama personāla iesaistīšanās un turpmāka analīze. Šos apstākļus attiecībā uz vienumiem var noteikt, izmantojot elementus no:

a) paredzētās funkcionālās bāzes līnijas – iesaistīties noviržu no paredzētās sistēmas funkcionālās darbības noteikšanā (izņemot informācijas drošības funkcijas / kontroles pasākumus);

b) paredzētās informācijas drošības bāzes līnijas – iesaistīties noviržu no paredzētās informācijas drošības kontroles pasākumu darbības noteikšanā attiecībā uz informācijas drošību.

Šajos apstākļos ir jāņem vērā gan normai neatbilstoša darbība, gan būtiskas novirzes no bāzes līnijām un attiecīga korelācija starp vairākiem neatkarīgiem notikumiem.

Papildu norādījumi par atklāšanas stratēģijas izveides mērķiem ir sniegti *EUROCAE* dokumenta ED-206 4. nodaļā.

## AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) apakšpunktu

**a) INCIDENTI**

Nosakot atbilstību IS.I.OR.220. punkta b) apakšpunktā minētajiem mērķiem attiecībā uz incidentiem, organizācijai ir jāņem vērā šādi aspekti:

1) procedūru sagatavošana un funkciju un pienākumu sadale, lai savlaicīgi, efektīvi un pienācīgi reaģētu uz visiem attiecīgajiem informācijas drošības incidentiem;

2) reaģēšanas procedūrā ir:

i) jāņem vērā brīdinājumi (gan atsevišķie, gan kombinētie), kas sniegti saskaņā ar IS.I.OR.220. punkta a) apakšpunkta 2) daļu un sadarbībā ar attiecīgo personālu jānovērtē to iespējamā ietekme uz aviācijas drošumu;

ii) atbilstoši IS.I.OR.220. punkta a) apakšpunkta 2) daļai jānosaka ierobežošanas stratēģija katrai aktīvu kategorijai, ņemot vērā iespējamo nelabvēlīgāko ietekmi un uzdevuma ierobežojumus, un jānodrošina kritēriji, kas norāda, ka incidents ir ierobežots;

iii) atbilstoši IS.I.OR.220. punkta b) apakšpunkta 3) daļai jānosaka pieņemamā ietekme uz katra tvērumā ietilpstošā aktīva drošumu un informācijas drošību, ja apdraudējuma scenārija īstenošanās gadījumā notiek to atteice;

3) reaģēšanas laikam ir jābūt samērīgam ar novērtēto ietekmes līmeni, kas minēts iepriekš 2) daļas iii) punktā;

4) reaģēšanas pasākumiem, kas īstenoti atbilstoši IS.I.OR.220. punkta b) apakšpunktam, jābūt balstītiem uz iepriekš a) apakšpunkta 2) daļā minēto reaģēšanas procedūru un jo īpaši tajos jāņem vērā:

i) maksimālā pieņemamā drošuma līmeņa pazemināšanās aktīviem incidenta mērogā;

ii) darbības, piemēram, pretestība, ierobežošana, maldināšana un iespējamo sistēmu atteices veidu kontrolēšana, kas palīdzēs sasniegt i) punktā noteikto pieņemamo drošuma līmeņa pazemināšanos, vienlaikus līdz minimumam samazinot ietekmi uz darbībām;

iii) resursi, kas nepieciešami ii) punktā minēto darbību īstenošanai;

5) attiecībā uz reaģēšanas laiku un pasākumiem jāņem vērā iespējamā tūlītējā nelabvēlīgā ietekme uz drošumu, ja pasākums tiek īstenots, pirms ir pilnīgi pārbaudīts, ka tas neradīs tūlītēju papildu ietekmi uz drošumu.

**b) IEVAINOJAMĪBAS**

Nosakot atbilstību IS.I.OR.220. punkta b) apakšpunktā minētajiem mērķiem saistībā ar ievainojamībām, organizācijai ir jāņem vērā šādi aspekti:

1) jāizveido ievainojamību pārvaldības stratēģija, kurā noteiktas procedūras, funkcijas un pienākumi, lai savlaicīgi, efektīvi un pienācīgi reaģētu uz visām atklātajām būtiskajām ievainojamībām;

2) reaģēšanas pasākumiem, kas īstenoti atbilstoši IS.I.OR.220. punkta b) apakšpunktam, jābūt balstītiem uz ievainojamības tvērumā ietilpstošo vienumu maksimālo pieņemamo risku, ņemot vērā nelabvēlīgāko ievainojamības izmantošanas scenāriju;

3) reaģēšanas laikam jābūt samērīgam ar brīdinājumu iepriekšēju izskatīšanu un ievainojamības iespējamās ietekmes novērtējumu, ja tā tiek izmantota.

## GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) apakšpunktu

Uzbrukumu uzskata par ierobežotu (t. i., tas neizplatās tālāk), ja ir noteiktas incidenta robežas un apdraudējums neizplatās ārpus šīm robežām. Papildu norādījumi ir sniegti *EUROCAE* dokumenta ED-206 5. nodaļā.

Termins “brīdinājums”, kas lietots IS.OR.220. punktā, nozīmē brīdinājumu, par kuru informācijas drošības notikumu pārvaldības vienībai jābūt laikus informētai un uz kuru tai jāreaģē.

Saistībā ar informācijas drošības reaģēšanas pasākumiem “maldināšana” ir virkne paņēmienu, kuru mērķis ir maldināt iespējamos uzbrucējus vai ļaunprātīgos lietotājus, lai tādējādi aizsargātu sistēmu un tās datus. Maldināšanas paņēmieni, piemēram, urķuslazdi vai atpakaļceļš ir radīti nolūkā maldināt, palēnināt vai novirzīt uzbrucējus, tādējādi palielinot to izmaksas un risku, vienlaikus nodrošinot aizsargiem vērtīgu laiku un izlūkdatus.

Norādījumi par ievainojamību pārvaldības stratēģiju ir sniegti *EUROCAE* dokumenta ED-206 3.4. nodaļā “Ievainojamību pārvaldības apsvērumi”. Tas nav vienīgais avots, kur var iegūt norādījumus, un organizācija var izmantot citus norādījumus, kas ir atbilstošāki tās vajadzībām.

## AMC1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” c) apakšpunktu

Nodrošinot atbilstību IS.I.OR.220. punkta c) apakšpunkta prasībai, organizācijai ir jāizstrādā incidenta seku novēršanas procedūra, kurā ir ietverti vismaz šādi elementi:

a) to aktīvu saraksts, kuri sniedz iespēju veikt drošu darbību, kā arī to savstarpējā atkarība, kas veido seku novēršanas tvērumu;

b) procesa apraksts ar nepieciešamajām prioritārajām darbībām, kas jāveic, lai seku novēršanas ietvaros atjaunotu drošu un neapdraudētu aktīvu stāvokli;

c) resursi, kas vajadzīgi b) apakšpunktā noteikto darbību veikšanai, lai nodrošinātu, ka šie resursi ir viegli pieejami pēc incidenta;

d) seku novēršanas laika mērķi, kas jānosaka attiecībā uz seku novēršanas tvērumā ietilpstošo aktīvu drošuma kritiskumu.

## GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” b) un c) apakšpunktu

**SEKU NOVĒRŠANAS MĒRĶI UN LAIKS**

IS.I.OR.220. punkta b) apakšpunktā ir aprakstīti notikumu apstākļi, kuri var kļūt vai ir kļuvuši par informācijas drošības incidentiem, kas var ietekmēt aviācijas drošumu, un attiecībā uz kuriem nepieciešams, lai būtu ieviesti reaģēšanas un seku novēršanas pasākumi, lai nodrošinātu, ka ekspluatācijas drošums saglabājas virs minimālā pieņemamā līmeņa.

Darbību un drošuma līmenis var būt savstarpēji saistīti, tāpēc dažos gadījumos, kad darbību līmeni apdraud informācijas drošības incidents un tas pazeminās, arī drošuma līmenis pazeminās. Tas skar, piemēram, gaisa satiksmes vadību; ja gaisa satiksmes pakalpojumu apjoms tiek samazināts vai tie kļūst neuzticami, samazinās arī lidojumu drošums.

Tomēr citos gadījumos saistība starp darbību līmeni un drošumu var būt apgriezta vai arī tie var būt neatkarīgi, līdz ar to, ja notiek incidents un darbību līmenis pazeminās, drošuma līmenis nemainās. Viens piemērs ir apdraudēts programmatūras ielādes process lidaparātā. Šādā gadījumā incidents, kas tiek atklāts un kam seko lēmums pārtraukt programmatūras ielādi, saglabātu pašreizējo drošuma līmeni.

Turpmāk 1. attēlā parādīta konceptuāla sistēma, ko var izmantot, lai noteiktu reaģēšanas un seku novēršanas mērķus, tostarp seku novēršanas laiks. Tas parāda, kā nelabvēlīgākā scenārija gadījumā paredzamais procesa vai darbības ekspluatācijas drošuma līmenis (drošuma līmenis) var mainīties laika gaitā, ja notiek informācijas drošības incidents. Šādā scenārijā drošuma līmeni vispirms pazemina incidents, bet pēc tam ar laiku tas pats turpina pazemināties. Šis attēls arī parāda gaidāmo ietekmi, kādai ir jāpiemīt mazināšanas pasākumiem un kontroles pasākumiem, proti, tiem ir jāierobežo ekspluatācijas drošuma pazemināšanās, tiklīdz notiek incidents, un jāuzlabo seku novēršana, t. i., atgriešanās paredzētajā drošuma līmenī.



|  |
| --- |
| **Laiks** |
| **1. attēls. Konceptuāla sistēma reaģēšanas un seku novēršanas mērķu noteikšanai** |

Kā tika norādīts, starp darbību līmeni un drošumu var būt dažādas attiecības, kuru dēļ atšķirtos iepriekšējā attēlā sniegtais atspoguļojums. Noteiktos gadījumos incidentam var būt aizkavēta ietekme uz drošuma līmeni (piemēram, kompromitēta izstrādes vide), kā parādīts 2. attēlā, vai arī tam var nebūt ietekmes, ja to pienācīgi kontrolē, kā tas ir iepriekš minētā kompromitētā programmatūras ielādes procesa gadījumā, kas parādīts 3. attēlā.

****

|  |  |
| --- | --- |
| **Laiks** | **Laiks** |
| **2. attēls. Incidents ar aizkavētu ietekmi uz drošumu** | **3. attēls. Incidents ar pilnīgi samazinātu ietekmi uz drošumu** |

Turklāt jāņem vērā, ka var būt dažādi veidi, kā risināt vienu un to pašu incidentu, jo drošumu var ietekmēt vairāki faktori.

Praktiski seku novēršanas laika mērķus, kas minēti AMC1 par IS.I.OR.220. punkta c) apakšpunktu, var izteikt kā to resursu un pakalpojumu sarakstu, kuri jāatjauno prioritārā secībā seku novēršanas ietvaros. Norādījumi par seku novēršanas laika mērķiem ir sniegti *EUROCAE* dokumenta ED-206 7.3.5. nodaļā.

## GM1 par IS.I.OR.220. punkta “Informācijas drošības incidenti – atklāšana, reaģēšana un seku novēršana” c) apakšpunktu

Seku novēršanas procedūrā vai seku novēršanas plānā jāapraksta incidentu seku novēršanas darbības un iesaistītie iekšējie vai ārējie resursi (piemēram, personāls, IT, ēkas, pakalpojumu sniedzēji). Norādījumi par incidentu seku novēršanas plānu ir sniegti *EUROCAE* dokumenta ED-206 7. nodaļā “Seku novēršana”.

Resursiem, kas vajadzīgi, lai piemērotu seku novēršanas pasākumus, jābūt pieejamiem, lai pēc incidenta savlaicīgi īstenotu seku novēršanas darbības. Šie resursi var būt pieejami iekšēji, vai arī tos var nodrošināt nolīgtās organizācijas, kā paredzēts IS.I.OR.235. punktā. Līgumi par seku novēršanas darbībām jānoslēdz pirms incidenta (preventīvi), un līgumā jāiekļauj noteikumi par to, ka nolīgtajai pusei ir savlaicīgi jāreaģē.

Droša un neapdraudēta stāvokļa atjaunošanai sākotnēji var būt nepieciešami ārkārtas pasākumi, kas ir darbības, kuras tiek uzsāktas, pamatojoties uz labāko attiecīgajā brīdī pieejamo informāciju, pirms tiek gūta pilnīga izpratne par situāciju, un šie pasākumi var pasliktināt pakalpojuma vai funkcionalitātes līmeni. Droša un neapdraudēta stāvokļa atjaunošana jāizvērtē, salīdzinot to ar sākotnējo riska novērtējumu, un tā drīkst tikai īslaicīgi atšķirties no parastajiem darbības apstākļiem. Tomēr atlikušā riska pieaugums un šā riska pieauguma ilgums, t. i., ārkārtas pasākumu īstenošanas dēļ, jādokumentē un jāpieņem pareizajā pārskatatbildības līmenī.

Šeit minētie seku novēršanas pasākumi var būt arī rezultāts reakcijai uz incidentiem, par kuriem organizācija ir saņēmusi informāciju, ka ir nepieciešams īstenot atbilstošus pasākumus, lai reaģētu uz informācijas drošības incidentiem vai uz ievainojamībām, kas var ietekmēt aviācijas drošumu.

Šādos apstākļos organizācijai var nebūt pieejams process vai seku novēršanas plāns, kas ietvertu konkrēto atgadījumu. Tāpēc organizācijai parasti ir jānosaka konkrēts seku novēršanas plāns, un parasti tam ir nepieciešams kompetentās iestādes apstiprinājums.

## AMC1 par IS.I.OR.225. punktu “Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem”

Atbilstība IS.I.OR.225. punktam jāpārvalda atbilstoši tam, kā katrai organizācijai paredzēts attiecīgajā īstenošanas regulā attiecībā uz jomu, kas minēta Regulas (ES) 2023/203 2. panta 1. punktā, saistībā ar reaģēšanu uz kompetentās iestādes paziņotajiem konstatējumiem. Jomas regulā var būt noteikts, ka organizācijai ir jāreaģē uz konstatējumiem atbilstoši to iedalījumam kategorijās.

## GM1 par IS.I.OR.225. punktu “Reaģēšana uz kompetentās iestādes paziņotajiem konstatējumiem”

Prasība par konstatējumu iedalījumu kategorijās un laika posmu, kurā jāveic IS.I.OR.225. punkta a) apakšpunktā minētās darbības, ir noteikta attiecīgās jomas īstenošanas regulas sadaļā “Prasības iestādēm”. Lai atklātu ar šo regulu saistītos konstatējumus, kompetentā iestāde ievēros iepriekš minēto prasību.

## GM1 par IS.I.OR.230. punktu “Sistēma ārējai ziņošanai par informācijas drošību”

Organizācijām ir jāziņo par atgadījumiem savai kompetentajai iestādei.

**PIEMĒRI**

*EASA* apstiprinātās projektēšanas organizācijas: *EASA* ir kompetentā iestāde.

Dalībvalsts kompetentās iestādes sertificēti aviopārvadātāji: dalībvalsts kompetentā iestāde ir kompetentā iestāde.

**ĪPAŠI GADĪJUMI**

Situācijā, kad organizācijai ir divi lidaparāta ekspluatanta sertifikāti (*AOC*) divās dažādās ES dalībvalstīs (A valstī un B valstī), par atgadījumiem, kuros iesaistīts lidaparāts, kas darbojas ar A valsts *AOC*, jāpaziņo A valsts kompetentajai iestādei, bet par atgadījumiem, kuros iesaistīts lidaparāts, kas darbojas ar B valsts *AOC*, jāziņo B valsts kompetentajai iestādei.

Ja organizācijai ir vairāki apstiprinājumi, jāziņo tās organizācijas apstiprinātās daļas kompetentajai iestādei, kurā ir noticis incidents vai ir atklāta ievainojamība. Ja incidents/ievainojamība ietekmē vairākus apstiprinājumus, tiks ziņots visām kompetentajām iestādēm.

Organizācijām, kam ir apstiprinājums, bet kas darbojas ārpus ES (piemēram, 145. daļa), kompetentā iestāde ir *EASA*, un tām ir jāziņo šai aģentūrai.

Divējāda lietojuma lidaparāti – par ievainojamību var būt jāziņo gan militārajās, gan civilajās ziņošanas sistēmās, ja tā ietekmē divējāda lietojuma funkciju/sistēmu. Informācija, kas tiek sniegta, izmantojot civilo ziņošanas sistēmu, ir jāattīra (t. i., visa sensitīvā informācija ir pienācīgi jāizdzēš).

## AMC1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

Lai nodrošinātu atbilstību IS.I.OR.230. punkta a) un b) apakšpunkta noteikumiem, organizācijai jāziņo:

a) par ikvienu atgadījumu, kas ietilpst Regulas (ES) Nr. 376/2014 darbības jomā un kas radies tīšas neatļautas elektroniskās mijiedarbības rezultātā;

b) par informācijas drošības incidentiem, kas var būtiski apdraudēt aviācijas drošumu un neietilpst Regulas (ES) Nr. 376/2014 darbības jomā;

c) par ievainojamībām, kas rada būtisku apdraudējumu aviācijas drošumam un vēl nav pienācīgi samazinātas atbilstoši apstiprinātai ievainojamības pārvaldības stratēģijai (skat. AMC1 par IS.I.OR.220. punkta b) apakšpunktu).

No iepriekšminētajiem ziņojumiem kompetento iestāžu pienākums saskaņā ar *IS* daļu ir nodrošināt atbilstību šīs regulas 7. pantam un iesniegt visu attiecīgo informāciju, kas jānodod saskaņā ar Direktīvas (ES) 2016/1148 8. pantu izraudzītajām informācijas drošības kompetentajām iestādēm.

## GM1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” a) un b) apakšpunktu

**SAISTĪBA STARP IS.I.OR.230. PUNKTA b) APAKŠPUNKTU UN REGULU (ES) Nr. 376/2014**

Eiropas Parlamenta un Padomes Regulā (ES) Nr. 376/2014 ir noteiktas prasības attiecībā uz ziņošanu par atgadījumiem civilajā aviācijā, to analīzi un turpmākajiem pasākumiem. Atbilstība IS.I.OR.230. punkta b) apakšpunktam neatbrīvo organizācijas no Regulas (ES) Nr. 376/2014 prasību izpildes.

Attiecībā uz katru ziņotāju kategoriju Regulā (ES) Nr. 2015/1018 ir noteikts to atgadījumu veids, par kuriem obligāti jāziņo. Regulā (ES) Nr. 376/2014 apspriesta arī brīvprātīga ziņošana par citiem atgadījumiem, kurus ziņotājs uzskata par aviācijas drošuma apdraudējumu.

Turklāt atbilstība Regulai (ES) Nr. 376/2014 neatbrīvo organizācijas no IS.I.OR.230. punkta b) apakšpunkta ievērošanas. Tomēr tas nenozīmē, ka ir jāveido divas paralēlas ziņošanas sistēmas, un šajā saistībā IS.I.OR.230. punkta b) apakšpunkts un Regula (ES) Nr. 376/2014 ir jāuzskata par savstarpēji papildinošiem.

Praksē tas nozīmē, ka IS.I.OR.230. punkta b) apakšpunktā paredzētie ziņošanas pienākumi ir saderīgi ar Regulā (ES) Nr. 376/2014 paredzētajiem ziņošanas pienākumiem. Šos ziņošanas pienākumus var izpildīt, izmantojot vienu ziņošanas kanālu. Turklāt jebkura fiziska vai juridiska persona, kam ir vairāk nekā viena funkcija, uz kuru attiecas ziņošanas pienākums, var izpildīt visus šos pienākumus, iesniedzot vienu ziņojumu. Organizācijas tiek aicinātas to pienācīgi aprakstīt organizācijas rokasgrāmatā, lai risinātu gadījumus, kad pienākumi tiek pildīti organizācijas vārdā.

**TURPMĀKA ANALĪZE**

Ja atbilstoši Regulai (ES) Nr. 376/2014 paziņota atgadījuma analīzē vēlāk tiek konstatēts, ka atgadījuma galvenais cēlonis vai veicinošais faktors ir bijusi tīša neatļauta elektroniskā mijiedarbība, organizācijai ir jāatjaunina savs paziņojums kompetentajai iestādei.

**BŪTISKS RISKS AVIĀCIJAS DROŠUMAM**

Saskaņā ar Regulas (ES) Nr. 376/2014 2. panta 7. punktā sniegto atgadījuma definīciju par ziņojamu atgadījumu ir jāuzskata ikviens informācijas drošības incidents vai ievainojamība, kas var radīt ievērojamu risku aviācijas drošumam. Ievērojams risks aviācijai nozīmē nedrošu stāvokli, t. i., tādu, kas var izraisīt nelaimes gadījumu vai nopietnu incidentu (kas noteikts *ICAO* 13. pielikumā).

Piezīme. Novērtējot iespējamību, ka informācijas drošības incidenta sekas var radīt nedrošu stāvokli, organizācijai jāapsver seku kombinācija, ja incidents skar vairākas sistēmas; daži pieņēmumi par sistēmu neatkarību, kas var atbilst patiesībai saistībā ar nejaušiem atgadījumiem, var nebūt spēkā apzinātu darbību gadījumā.

**SAISTĪBA STARP IS.I.OR.230. PUNKTA b) APAKŠPUNKTA 1) DAĻU UN CITĀM AR AVIĀCIJAS PRODUKTIEM VAI DAĻĀM SAISTĪTU INFORMĀCIJAS DROŠĪBAS ATGADĪJUMU ZIŅOŠANAS PRASĪBĀM**

Attiecībā uz organizācijām, uz kurām attiecas ar aviācijas produktiem vai daļām saistītu informācijas drošības atgadījumu ziņošanas prasības, uzskata, ka atbilstība konkrētajiem īstenošanas regulas noteikumiem to jomā ir pietiekama, lai nodrošinātu atbilstību IS.I.OR.230. punkta b) apakšpunkta 1) daļas prasībām. Piemēram, attiecībā uz organizācijām, uz kurām attiecas Regula (ES) Nr. 748/2012, ziņošanu var veikt saskaņā ar minētās regulas I pielikuma (21. daļas) 21.A.3A punktu.

## AMC1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” c) apakšpunktu

Kopējā 72 stundu laika ierobežojuma ietvaros ziņojuma iesniegšanas steidzamības pakāpe jānosaka atkarībā no tā, cik liela ietekme uz drošību tiek uzskatīta par informācijas drošības incidenta vai atklātās ievainojamības izraisītu. Ja persona, kas nosaka iespējamo nedrošo stāvokli, uzskata, ka atgadījums ir izraisījis tūlītēju un īpaši būtisku apdraudējumu, kompetentā iestāde sagaida, ka tai nekavējoties un ar iespējami ātrākajiem līdzekļiem (pa tālruni, faksu, e-pastu, teleksu utt.) tiks paziņota visa attiecīgajā brīdī pieejamā informācija.

## GM1 par IS.I.OR.230. punkta “Sistēma ārējai ziņošanai par informācijas drošību” c) apakšpunktu

Norādījumi par informācijas drošības incidentu un ievainojamību ziņošanu ir sniegti *EUROCAE* dokumenta ED-206 6.4.2.2. nodaļā “Ziņošanas grafiks” un 6.4.5. nodaļā “Ziņojamās informācijas saturs”. Tas nav vienīgais avots, kurā ir sniegti norādījumi, un organizācija var izmantot citus norādījumus, kas ir atbilstošāki tās vajadzībām.

Piezīme. Personai, kas ziņo par atgadījumu atbilstoši Regulai (ES) Nr. 376/2014, var nebūt iespēju noteikt atgadījuma veidu. Tas jo īpaši attiecas uz informācijas drošību, un rezultātu var iegūt no tiesu ekspertīzes, kurā noskaidro atgadījuma informācijas drošības veidu. Izvērtēšana notiks sākotnējā iekšējā ziņošanas procesa ietvaros (skat. IS.I.OR.215. punktu un saistītos *AMC*). Atgadījuma izvērtēšanā var tikt atklāta iespējamība, ka atgadījums radīs nedrošu stāvokli, ņemot vērā tā īstenošanās varbūtību.

## GM1 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana”

Organizācijas var nolemt nodot konkrētas darbības ārpakalpojumu sniedzējiem gan savu darbības vajadzību nodrošināšanai, gan nolūkā nodrošināt atbilstību šai regulai (informācijas drošības pārvaldības darbības). Darbības, par kurām noslēgti līgumi darbības vajadzību nodrošināšanai, var ietilpt *IS* daļas darbības jomā, tāpēc attiecīgie informācijas drošības riski ir jāpārvalda saskaņā ar IS.I.OR.205. un IS.I.OR.210. punkta prasībām. Savukārt uz informācijas drošības pārvaldības darbībām attiecas IS.OR.235. punkta īpašie noteikumi, jo ar šīm darbībām saistītie jautājumi var būtiski ietekmēt organizāciju.

Tāpēc IS.I.OR.235. punkta mērķi ir šādi:

a) aizsargāt būtisko un sensitīvo informāciju un aktīvus, kad ar tiem rīkojas organizācijas, kas nolīgtas informācijas drošības pārvaldības darbību nodrošināšanai (tostarp organizācijas piegādes ķēdē) vai nu to objektos, vai organizācijas objektos, vai kad tos pārsūta starp organizāciju un nolīgtajām organizācijām, vai kad tiem attālināti piekļūst nolīgtās organizācijas;

b) novērst, ka informācijas drošības riskus rada produkti un pakalpojumi, ko organizācijai izstrādājušas vai sniegušas nolīgtās organizācijas informācijas drošības pārvaldības darbību nodrošināšanas ietvaros;

c) nodrošināt, ka informācijas drošības riski tiek pārvaldīti visos attiecību ar nolīgtajām organizācijām posmos.

## GM2 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana”

a) Informācijas drošības pārvaldības darbību līguma slēgšana ir paņēmiens, kā līgumslēdzēja organizācija var nodot uzdevumus izpildei trešajām personām (nolīgtajām organizācijām). Līgumslēdzējai organizācijai joprojām ir pienākums pārraudzīt nolīgtās(-o) organizācijas(-u), un tā atbild par šīs regulas ievērošanu.

b) Līgums var būt rakstiska vienošanās, vienošanās dokuments, pakalpojumu līgums, saprašanās memorands utt. atbilstoši nolīgtajām darbībām.

## GM3 par IS.I.OR.235. punktu “Informācijas drošības pārvaldības darbību līguma slēgšana”

**PIEMĒRI**

Turpmāk 1. tabulā sniegti daži piemēri informācijas drošības pārvaldības darbībām, par kurām var slēgt līgumus atbilstoši IS.I.OR.200. punkta noteikumiem.

**1. tabula. Piemēri informācijas drošības pārvaldības darbībām, par kurām var slēgt līgumus**

| **Ar darbībām saistītie IS.I.OR.200. punkti** | **Nolīgtās darbības piemērs** |
| --- | --- |
| a) apakšpunkta 1) daļa: izveido informācijas drošības politiku, kurā izklāstīti organizācijas vispārējie principi attiecībā uz informācijas drošības risku iespējamo ietekmi uz aviācijas drošumu. | Informācijas drošības politikas plānošana un konsultācijas. |
| a) apakšpunkta 2) daļa: identificē un pārskata informācijas drošības riskus saskaņā ar IS.I.OR.205. punktu. | Noteikt darbības, objektus un resursus.Noteikt saskarnes ar citām organizācijām, kuras varētu būt pakļautas informācijas drošības riskiem.Veikt pilnīgu vai daļēju riska analīzi, piemēram, noteikt un klasificēt informācijas drošības riskus. |
| a) apakšpunkta 3) daļa: nosaka un īsteno informācijas drošības riska risināšanas pasākumus saskaņā ar IS.I.OR.210. punktu. | Noteikt, izstrādāt un īstenot pasākumus.Pārbaudīt īstenoto pasākumu sākotnējo un pastāvīgo rezultativitāti (piemēram, sarkanās komandas / zilās komandas mācības, iespiešanās pārbaude, ievainojamību skenēšana utt.).Paziņot iesaistītajām ieinteresētajām personām riska novērtējuma rezultātus un to pienākumus riska risināšanas procesā. |
| a) apakšpunkta 4) daļa: īsteno sistēmu iekšējai ziņošanai par informācijas drošību saskaņā ar IS.I.OR.215. punktu. | Noteikt, izstrādāt un īstenot iekšējās ziņošanas sistēmu, lai varētu apkopot un izvērtēt informācijas drošības notikumus un iekārtu, procesu un pakalpojumu ievainojamību. |
| a) apakšpunkta 5) daļa: saskaņā ar IS.I.OR.220. punktu nosaka un īsteno pasākumus, kas vajadzīgi, lai atklātu informācijas drošības notikumus, identificē tos notikumus, kas uzskatāmi par incidentiem, kuri spēj ietekmēt aviācijas drošumu, neskarot izņēmumus, kas atļauti saskaņā ar IS.I.OR.205. punkta e) apakšpunktu, reaģē uz minētajiem informācijas drošības incidentiem un novērš to sekas. | Noteikt, izstrādāt un īstenot pasākumus notikumu atklāšanai.Noteikt, izstrādāt un īstenot pasākumus, lai reaģētu uz jebkādiem notikumu apstākļiem.Noteikt, izstrādāt un īstenot pasākumus, kuru mērķis ir novērst informācijas drošības incidentu sekas. |
| a) apakšpunkta 6) daļa: īsteno kompetentās iestādes paziņotos pasākumus kā tūlītēju reakciju uz informācijas drošības incidentu vai ievainojamību, kas ietekmē aviācijas drošumu. | Īstenot tūlītējus pasākumus reaģēšanai uz informācijas drošības incidentu vai ievainojamību, par ko ir paziņojusi kompetentā iestāde. |
| a) apakšpunkta 7) daļa: lai reaģētu uz kompetentās iestādes paziņotajiem konstatējumiem, veic atbilstīgus pasākumus saskaņā ar IS.I.OR.225. punktu. | Noteikt galveno cēloni.Noteikt korektīvo pasākumu plānu.Sniegt pierādījumus par korektīvajiem pasākumiem, kas īstenoti, lai novērstu neatbilstības. |
| a) apakšpunkta 8) daļa: lai kompetentā iestāde varētu veikt atbilstīgus pasākumus, īsteno ārējās ziņošanas sistēmu saskaņā ar IS.I.OR.230. punktu. | Noteikt, izstrādāt un īstenot ārējās ziņošanas sistēmu, lai kompetentajai iestādei un, ja nepieciešams, projekta apstiprinājuma turētājam vai par projektu atbildīgajai organizācijai varētu paziņot par informācijas drošības incidentiem un par iekārtu, procesu un pakalpojumu ievainojamību. |
| a) apakšpunkta 9) daļa: ja tiek slēgts līgums ar citām organizācijām par jebkuru daļu no IS.I.OR.200. punktā aprakstītajām darbībām, nodrošina atbilstību IS.I.OR.235. punktā ietvertajām prasībām. | Nav piemērojams. |
| a) apakšpunkta 10) daļa: nodrošina atbilstību prasībām, kas IS.I.OR.240. punktā noteiktas attiecībā uz personālu. | Atbildīgā vadītāja darbības saskaņā ar noteikumiem par “kopīgu atbildīgo personu”, kas minēta IS.I.OR.240. punktā.Atbilstības uzraudzība, kā paredzēts IS.I.OR.240. punktā.Nolīgta organizācija, lai nodrošinātu, ka ar šo regulu saistīto darbību īstenošanai ir norīkots pietiekams personāls.Noteikt, izstrādāt un nodrošināt atbilstošas mācības, lai sasniegtu nepieciešamo personāla kompetenci.Veikt pārbaudes pirms pieņemšanas darbā. |
| a) apakšpunkta 11) daļa: nodrošina atbilstību IS.I.OR.245. punktā ietvertajām reģistrācijas prasībām. | Noteikt, izstrādāt un veikt drošu arhivēšanu.Nodrošināt drošu datu centru (kā pakalpojumu). Nodrošināt ierakstu atjaunināšanu. |
| a) apakšpunkta 12) daļa: uzrauga organizācijas atbilstību šīs regulas prasībām un sniedz atsauksmes par konstatējumiem atbildīgajam vadītājam, lai nodrošinātu korektīvo pasākumu efektīvu īstenošanu. | Atbilstības uzraudzība (kas paredzēta IS.I.OR.240. punktā), tostarp neatkarīgu revīziju īstenošana. |
| a) apakšpunkta 13) daļa: neskarot ziņošanai par incidentiem piemērojamās prasības, aizsargā jebkuras tādas informācijas konfidencialitāti, ko organizācija, iespējams, ir saņēmusi no citām organizācijām, atkarībā no tās sensitivitātes līmeņa. | Noteikt, izstrādāt un īstenot risinājumus jebkādas informācijas konfidencialitātes aizsardzībai. |
| b) apakšpunkts: lai nodrošinātu pastāvīgu atbilstību 1. pantā minētajām prasībām, organizācija īsteno pastāvīgu uzlabojumu procesu saskaņā ar IS.I.OR.260. punktu. | Veikt neatkarīgus rezultativitātes un gatavības novērtējumus.Noteikt, izstrādāt un īstenot nepieciešamos uzlabošanas pasākumus. |
| c) apakšpunkts: organizācija saskaņā ar IS.I.OR.250. punktu dokumentē visus galvenos procesus, procedūras, funkcijas un pienākumus, kas vajadzīgi, lai izpildītu IS.I.OR.200. punkta a) apakšpunkta prasības, un izveido minētās dokumentācijas grozījumu veikšanas procesu. Šo procesu, procedūru, funkciju un pienākumu izmaiņas pārvalda saskaņā ar IS.I.OR.255. punktu. | Sagatavot dokumentāciju, lai sīki atspoguļotu visus galvenos procesus, procedūras, funkcijas un pienākumus, kas nepieciešami, lai nodrošinātu atbilstību IS.I.OR.200. punkta a) apakšpunktam (piemēram, informācijas drošības politika, vispārīgs personāla apraksts, atbilstības noteikšanas procedūras).Noteikt, izstrādāt un īstenot procesus grozījumu un izmaiņu apstiprināšanai. |

## AMC1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu

**a) NOLĪGTĀS ORGANIZĀCIJAS PĀRRAUDZĪBA**

Lai īstenotu nolīgtās organizācijas pārraudzību, organizācijai atbilstoši *IS* daļai ir jābūt:

1) procesam, ar kuru nodrošina atbilstību šīs regulas noteikumiem attiecībā uz nolīgtajām darbībām;

2) strukturētam procesam paredzētās līguma izpildes uzraudzībai, kas ietver:

i) darbību tvēruma noteikšanu un vienošanos par to;

ii) pušu (t. i., līgumslēdzējas organizācijas un nolīgtās organizācijas) funkciju un pienākumu noteikšanu;

iii) galveno darbības rādītāju noteikšanu un pārskatīšanu;

iv) reaģēšanu uz atkāpšanos no līgumsaistību izpildes;

v) atbilstības revīziju veikšanu saskaņā ar iepriekš noteikto tvērumu un mērķiem, lai izvērtētu darbības pasākumus un saistītos nodrošināšanas pasākumus;

vi) atgriezeniskās saites sniegšanu par atbilstības revīziju rezultātiem gan organizācijā, gan nolīgtajā organizācijā un reaģēšanu uz konstatējumiem. Atgriezeniskajai saitei par atbilstības revīziju rezultātiem līgumslēdzējā organizācijā ir jānonāk pie atbildīgā vadītāja vai deleģētās(-ajām) personas(-ām), lai nodrošinātu pienācīgu reaģēšanas uz konstatējumiem (t. i., korektīvo pasākumu īstenošanas) uzraudzību vai līguma darbības izbeigšanu, ja tas tiek uzskatīts par vajadzīgu.

Piezīme. Pušu noslēgtajā līgumā ir jābūt noteiktām organizācijas tiesībām veikt nolīgtās organizācijas atbilstības revīzijas.

**b) AR NOLĪGTAJĀM DARBĪBĀM SAISTĪTO RISKU PĀRVALDĪBA**

Lai pienācīgi pārvaldītu riskus, kas ir saistīti ar nolīgtajām darbībām, organizācijai jānodrošina atbilstība šādiem kritērijiem:

1) pirms jebkādu informācijas drošības pārvaldības darbību nodošanas ārpakalpojumu sniedzējiem tiek veikts iepriekšējs piegādātāju novērtējums. Novērtējumā jāizvērtē pakalpojuma sniedzēja kompetences, ilgtspējība, kā arī kvalifikācija saistībā ar nolīgstamajām darbībām;

2) ir novērtēti riski saistībā ar to nolīgto darbību nodrošināšanu, par kurām organizācija ir vienojusies ar nolīgto organizāciju atbilstoši *IS* daļai;

3) organizācija izveido un uztur atbilstošus kanālus saziņai ar nolīgto organizāciju par informācijas drošības jautājumiem.

## GM1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu

**IEPRIEKŠĒJS NOVĒRTĒJUMS**

Iepriekšējo novērtējumu veic, lai izvērtētu piegādātāju kompetenci, ilgtspējību, kā arī kvalifikācijas saistībā ar informācijas drošības darbībām, par kurām paredzēts noslēgt līgumu. Veicot šo iepriekšējo novērtējumu, iespējams, būs jāņem vērā citas juridiskās prasības vai iepirkuma procedūras, ko piemēro kompetentajai iestādei, tāpēc to var veikt dažādos veidos, piemēram:

a) publisko piedāvājumu iepirkuma procedūras dokumentos iekļaujot atbilstības prasības potenciālajiem piegādātājiem;

b) izskatot informācijas drošības apliecinājumus, ko ārēji un neatkarīgi revidenti ir piešķīruši potenciālajiem piegādātājiem;

c) izskatot potenciālo piegādātāju sagatavotās pašnovērtējuma anketas.

**AR NOLĪGTO DARBĪBU NODROŠINĀŠANU SAISTĪTAIS RISKA NOVĒRTĒJUMS**

Riska novērtējumā jāņem vērā nolīgtās organizācijas gatavības līmenis un jāapsver šādi aspekti:

a) tādas būtiskas un sensitīvas informācijas un aktīvu noteikšana un novērtēšana, ko var sniegt ārpakalpojumu sniedzējiem vai saņemt no tiem;

b) nolīgtajai organizācijai piemērojamo organizācijas informācijas drošības prasību noteikšana;

c) izvērtējums par nolīgtās organizācijas (gan pašreizējo, gan jauno nolīgto organizāciju) spēju izpildīt līgumslēdzējas organizācijas informācijas drošības prasības, kas veikts, izmantojot pakalpojuma sniedzēja novērtēšanu;

d) to risku novērtēšana, kurus var radīt nolīgtā organizācija.

Šajā saskaņotajā riska novērtējumā jāizvērtē arī līgumslēdzējas un nolīgtās organizācijas funkcijas un pienākumi, kā arī to saskarnes.

## GM2 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana”a) apakšpunktu

**NOLĪGTO ORGANIZĀCIJU REVĪZIJA**

Veicot revīziju pakalpojumu sniedzējam, kas nolīgts informācijas drošības pārvaldības darbību veikšanai, organizācijai jāņem vērā šādi aspekti:

* revīzijas tvērums un mērķis ir jāattiecina tikai uz procesiem, resursiem (t. i., uz nolīgtās organizācijas personālu, sistēmām/aprīkojumu, tīkliem) un datiem, ko izmanto nolīgto *IS* daļas darbību veikšanai;
* atbilstības un/vai īstenošanas revīzijas jāveic pēc līgumslēdzējas organizācijas ieskatiem;
* revīzijas konstatējumi ir jārisina, izmantojot labojumu veikšanas plānu ar līgumslēdzējas organizācijas apstiprinātu termiņu.

## AMC1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana” b) apakšpunktu

Lai pēc pieprasījuma nodrošinātu kompetentās iestādes piekļuvi nolīgtajai organizācijai, organizācijai atbilstoši *IS* daļai ir jānodrošina, ka šāda prasība vai noteikums ir iekļauts līguma dokumentācijā.

Kompetentās iestādes piekļuvei nolīgtajām organizācijām jābūt vismaz līdzvērtīgai tai, kas piešķirta līgumslēdzējai organizācijai, un jebkurā gadījumā pietiekamai, lai nodrošinātu, ka tiek novērtēta līgumā paredzēto darbību pastāvīga atbilstība piemērojamajām prasībām.

## GM1 par IS.I.OR.235. punkta “Informācijas drošības pārvaldības darbību līguma slēgšana” b) apakšpunktu

Piekļuve nolīgtajai organizācijai nozīmē to, ka ir pieejami pierādījumi par nolīgto pasākumu atbilstību (piemēram, artefakti, dokumenti, neatkarīgi apliecinājumi).

Pierādījumus par atbilstību var iegūt, nododot dokumentus un/vai piekļūstot informācijai telpās saskaņā ar līgumā noteikto “revīzijas tvērumu”.

Gadījumos, kad organizācija nolīgto informācijas drošības pārvaldības pakalpojumu ietvaros izmanto komerciālus plašpatēriņa pakalpojumus ar līguma standartklauzulām, organizācijai jāapsver, vai šīs klauzulas nodrošina pietiekamu piekļuvi nepieciešamajai informācijai.

Iespēja apmeklēt telpas jāizvērtē, ņemot vērā dažādus aspektus, piemēram, saistītās informācijas sensitivitātes pakāpi vai praktisko pieejamību nolīgtajai organizācijai (piemēram, nolīgtā organizācija ir pakalpojumu sniedzējs ar dalītiem resursiem).

## GM1 par IS.I.OR.240. punktu “Prasības personālam”

Šā punkta a)–e) apakšpunktā ietverto prasību mērķi ir šādi:

a) nodrošināt, ka ir ieviesta efektīva organizatoriskā struktūra, lai nodrošinātu atbilstību šīs regulas prasībām;

b) sniegt pārliecību citām organizācijām, ar kurām tām ir kopīgi riski.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 2) daļu

**INFORMĒŠANA PAR INFORMĀCIJAS DROŠĪBAS POLITIKU**

Organizācijas atbildīgajam vadītājam jānodrošina, ka informācijas drošības politika ir zināma un viegli pieejama darbiniekiem atbilstoši viņu pienākumiem.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 3) daļu

**PAMATIZPRATNE PAR REGULU**

Lai apliecinātu pamatizpratni par šo regulu, organizācijas atbildīgajam vadītājam jāspēj izskaidrot regulas vispārējos mērķus un tās ietekmi uz organizāciju.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” a) apakšpunkta 3) daļu

**PAMATIZPRATNE PAR REGULU**

Ja atbildīgajam vadītājam nav iepriekšējas pieredzes ar *IS* daļu saistītajās darbības jomās, viņš var gūt vajadzīgo izpratni, apmeklējot mācības par regulas saturu un atbilstības nodrošināšanas tehnisko bāzi. Jo īpaši mācību materiālos jābūt apspriestiem *IS* daļas vispārējiem mērķiem, un novērtējumā jāizvērtē izpratne par šiem regulatīvajiem mērķiem.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” b) apakšpunktu

**PERSONAS VAI PERSONU GRUPAS IECELŠANA**

Personai vai personu grupai, kas iecelta saskaņā ar IS.I.OR.240. punkta b) apakšpunktu un kam ir pienākums nodrošināt atbilstību šīs regulas prasībām, jāpārstāv organizācijas vadības struktūra.

Personai vai personu grupai ir tieša piekļuve atbildīgajam vadītājam (vai kopīgajai atbildīgajai personai, ja tāda ir iecelta), lai sniegtu vadlīnijas, norādījumus un atbalstu procesa un standartu plānošanai, īstenošanai un darbībai nolūkā nodrošināt atbilstību šai regulai. Šīm personām jābūt tiešai piekļuvei atbildīgajam vadītājam (vai kopīgajai atbildīgajai personai), lai pienācīgi informētu attiecīgo vadītāju par atbilstības un informācijas drošības jautājumiem.

Ieceļot personu amatā, jāņem vērā iespējamība, ka persona kādu laiku var nespēt veikt tai uzticētos organizatoriskos uzdevumus, un tāpēc jāapzina arī nepieciešamie vietnieki.

Šīm ieceltajām personām jāpierāda, ka tās pilnīgi izprot šīs regulas prasības, lai spētu nodrošināt, ka organizācijas procesi un standarti precīzi atbilst piemērojamajām prasībām. Šo personu uzdevums ir nodrošināt, ka atbilstība tiek preventīvi pārvaldīta un visas agrīnās neatbilstības pazīmes tiek dokumentētas un uz tām tiek reaģēts.

IDPR jāiekļauj iecelto personu un vietnieku funkciju un pienākumu apraksts, tostarp jānorāda viņu vārdi un uzvārdi (skat. IS.I.OR.250. punkta a) apakšpunkta 2) daļu).

## GM1 par IS.I.OR.240. punkta “Prasības personālam” b) apakšpunktu

Ieceltas personas ilgstošas prombūtnes apstāklis iestājas tad, ja šī persona nespēj izpildīt tai uzticētos organizatoriskos pienākumus. Piemēram, ja ieceltajām personām noteiktā laika posmā ir jāveic informācijas drošības pārvaldības pasākums, prombūtne tiek uzskatīta par ilgstošu, ja tā pārsniedz šo laika posmu un ja tāpēc var rasties pārvaldības pasākuma ievainojamība.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” b) un c) apakšpunktu

Iecelšanu var veikt, izmantojot e-pastu, organigrammu, funkciju un pienākumu tabulu un citus līdzekļus, ko organizācija parasti izmanto. Organizācija var pieņemt jebkādus amata nosaukumus iepriekš minētajiem informācijas drošības vadības amatiem, bet tai ir jānorāda kompetentajai iestādei amata nosaukumi un personas, kas ir izvēlētas šo funkciju veikšanai.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” c) apakšpunktu

**ATBILSTĪBAS UZRAUDZĪBAS FUNKCIJA**

Persona, kas ir iecelta saskaņā ar IS.I.OR.240. punkta c) apakšpunktu un kam ir pienākums pārvaldīt atbilstības uzraudzības funkciju atbilstoši IS.I.OR.200. punkta a) apakšpunkta 12) daļai, var būt tā pati persona, kas ir atbildīga par atbilstības uzraudzības funkciju, kura noteikta īstenošanas regulā attiecībā uz konkrēto jomu, vai var ziņot šādai personai.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” d) apakšpunktu

**KOORDINĀCIJA**

Kritēriji, lai izveidotu koordināciju, kas nodrošina pienācīgu informācijas drošības pārvaldības integrāciju organizācijā, ir šādi:

a) ir noteikta organizāciju darbības joma un robežas, un par tām ir paziņots kopīgajai atbildīgajai personai;

b) šīs regulas prasības ir paziņotas un nodotas kopīgajai atbildīgajai personai;

c) kopīgajai atbildīgajai personai ir tieša piekļuve atbildīgajam vadītājam;

d) jautājumi tiek preventīvi pārvaldīti, un visas agrīnās neatbilstības pazīmes tiek dokumentētas un uz tām tiek reaģēts.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” e) apakšpunktu

**KOPĪGA ATBILDĪGĀ PERSONA**

Ja atbildīgais vadītājs deleģē šai regulai atbilstošu pasākumu izpildi kopīgai atbildīgajai personai, šai personai jāpiešķir arī atbilstošs pilnvarojums, kas vajadzīgs, lai īstenotu IS.I.OR.200. punkta noteikumus, tostarp tiesības un finanšu līdzekļi, lai mobilizētu un kontrolētu resursus visās organizācijās vai iesaistītās organizācijas daļās. Šajā pilnvarojumā var ietvert arī IS.I.OR.240. punkta b) un c) apakšpunktā minētās personas vai personu grupas iecelšanu, un kopumā kopīgajai atbildīgajai personai tās pienākumu izpildē var palīdzēt papildu personāls.

Iespēja deleģēt kopīgu atbildīgo personu ir pieejama organizācijai, kurai ir kopīgas informācijas drošības organizatoriskās struktūras, politika, procesi un procedūras ar citām organizācijām vai ar tās pašas organizācijas daļām, kas nav iekļautas atļaujā vai deklarācijā, un tāpēc tiek sagaidīts, ka šai kopīgajai atbildīgajai personai būs informācijas drošības pienākumi un kompetence. Jo īpaši kopīgajai atbildīgajai personai jāspēj pārvaldīt organizācijas informācijas drošības stratēģiju un tās īstenošanu, lai nodrošinātu 1. pantā aprakstīto mērķu sasniegšanu. Saskaņā ar *ENISA* 2022. gada septembrī publicēto Eiropas kiberdrošības prasmju sistēmu (*ECSF*) šo personu var dēvēt, piemēram, par (galveno) informācijas drošības speciālistu, kiberdrošības programmas direktoru vai informācijas drošības pārvaldnieku. Tomēr jāņem vērā, ka šajos aprakstos un ar tiem saistītajās prasmēs nav ņemta vērā aviācijas drošuma perspektīva, kas noteikta 1. pantā.

Ja struktūrai ir vairākas atļaujas vai deklarācijas, attiecīgie atbildīgie vadītāji var deleģēt to pašu kopīgo atbildīgo personu, kas tādējādi būs atbildīga par IS.I.OR.200. punkta noteikumu īstenošanu attiecībā uz funkcionālu klasteru ar kopīgām informācijas drošības struktūrām, politiku, procesiem un procedūrām.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” f) apakšpunktu

**PIETIEKAMS PERSONĀLS**

Lai noteiktu personāla pietiekamību, jāņem vērā šādi elementi:

a) organizatoriskās struktūras, politika, procesi un procedūras, uz kurām attiecas informācijas drošības pārvaldība;

b) nepieciešamā koordinācija ar citām organizācijām, līgumslēdzējiem un piegādātājiem;

c) riska līmenis, kas ir saistīts ar organizācijas veiktajiem pasākumiem.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” f) apakšpunktu

**PIETIEKAMS PERSONĀLS**

Šajā regulā personāls ir organizācijas tieši nodarbinātu darbinieku kopums, kā arī personāls, kas nolīgts atbilstoši IS.I.OR.235. punktam.

Veidojot organizatorisko struktūru, kas vajadzīga šīs regulas prasību izpildei, jāņem vērā II papildinājumā minētie pasākumi attiecībā uz galvenajiem uzdevumiem, kuri izriet no *IS* daļas īstenošanas.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” g) apakšpunktu

**NEPIECIEŠAMĀ KOMPETENCE**

a) Lai noteiktu kompetenci, kas nepieciešama personālam, kurš veic darbības, jāņem vērā šādi elementi:

1) darba pienākumi un saistītie uzdevumi;

2) nepieciešamās zināšanas, prasmes un spējas.

b) Lai nodrošinātu, ka personāls uztur nepieciešamo kompetenci, organizācijai procesa ietvaros:

1) jānovērtē personāla kvalifikācija un pieredze attiecībā uz uzticētajā amatā vajadzīgo kompetenci, lai konstatētu nepilnības;

2) darbinieku kvalifikācija un pieredze jāpielīdzina kompetencei, kas personālam nepieciešama, lai tas spētu izpildīt savas funkcijas, šajā nolūkā organizējot atbilstošas mācību programmas pašreizējiem darbiniekiem, pieņemot darbā jaunus resursus vai apvienojot šīs darbības;

3) jāuztur personāla kompetence laikā, kad tas ir norīkots izpildīt darba funkciju.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” g) apakšpunktu

**NEPIECIEŠAMĀ KOMPETENCE UN MĀCĪBU PROGRAMMA**

Mācību programmā vispirms ir jānosaka kompetence, kas personālam nepieciešama katras funkcijas nodrošināšanai, un pēc tam jānosaka atšķirības starp pašreizējo un nepieciešamo kompetenci.

Lai izstrādātu kompetenču sarakstu, organizācija kā sākotnējos norādījumus var izmantot jau izstrādātu kiberdrošības kompetences sistēmu, piemēram, Nacionālo iniciatīvu par izglītību kiberdrošības jomā (*National Initiative for Cybersecurity Education* – *NICE*), kuras pamatā ir *NIST* kiberdrošības sistēma (*NIST CSF*).

Šā dokumenta II papildinājumā ir uzskaitīti šajā regulā paredzētie galvenie uzdevumi un izkārtoti kopā ar kompetencēm, kas atvasinātas no *NIST CSF*. Šo kartējumu var izmantot, lai izveidotu bāzes līniju ar mērķi noteikt iepriekš minētās kompetences neatbilstības. Tomēr jāņem vērā, ka pašreizējās kiberdrošības / informācijas drošības kompetenču sistēmās, piemēram, *NICE*, galvenā uzmanība parasti ir pievērsta standarta informācijas tehnoloģiju aizsardzībai; tāpēc ierosinātais kompetenču saraksts var būt jāpielāgo tehnoloģijām vai jāintegrē organizācijā izmantotajos procesos.

Konstatēto neatbilstību novēršana jāpieņem kā mācību programmas mērķis, šajā saistībā nosakot arī tādu mācību apjomu, saturu, pasniegšanas metodes (piemēram, mācības klātienē, e-mācības, paziņojumi, mācības darbavietā) un biežumu, kas vislabāk atbilst organizācijas vajadzībām, ņemot vērā organizācijas lielumu, darbības jomu, nepieciešamās kompetences un sarežģītību.

Visbeidzot, informācijas drošībai / kiberdrošībai attīstoties jauna apdraudējuma parādīšanās dēļ, organizācijai ir periodiski jāpārskata mācību programmas piemērotība.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” h) apakšpunktu

**PIENĀKUMU APSTIPRINĀJUMS**

Attiecībā uz visām piešķirtajām funkcijām un uzdevumiem organizācijai skaidri un pārredzami jānorāda visi darbinieka pienākumi informācijas drošības jomā.

Šajā saistībā visam personālam, kas veic šajā regulā paredzētās darbības, izsekojamā un pārbaudāmā veidā jāapliecina izpratne par piešķirtajām funkcijām un ar tām saistītajiem pienākumiem informācijas drošības jomā.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” h) apakšpunktu

**PIENĀKUMU APSTIPRINĀJUMS**

Saņemšanas apstiprinājums, piemēram, ar derīgu elektronisko vai pašrocīgu parakstu, apstiprinājuma e-pasta ziņojumu u. tml., ir izsekojams apstiprinājuma pierādījums.

## AMC1 par IS.I.OR.240. punkta “Prasības personālam” i) apakšpunktu

**IDENTITĀTE UN UZTICAMĪBA**

Personāla, kam ir pieeja informācijas sistēmām un datiem, uz kuriem attiecas *IS* daļas prasības, identitāte jānosaka, pamatojoties uz dokumentāriem pierādījumiem.

Lai noteiktu šāda personāla uzticamību, organizācijai jābūt dokumentētam procesam un atbilstošiem kritērijiem, lai nodrošinātu, ka šīm personām var uzticēt attiecīgos amata pienākumus.

## GM1 par IS.I.OR.240. punkta “Prasības personālam” i) apakšpunktu

**IDENTITĀTE UN UZTICAMĪBA**

a) Uzticamību var noteikt, piemēram:

1) pirms pieņemšanas darbā veicot iepriekšējās darbības pārbaudi saskaņā ar piemērojamajiem Savienības un valsts tiesību aktiem. Šī pārbaude var ietvert šādu faktu apstiprināšanu:

i) izglītība, iepriekšējā nodarbinātība un jebkādas nepilnības iepriekšējos gados;

ii) sodāmības neesība;

iii) jebkura cita būtiska informācija vai izlūkdati, ko uzskata par būtiskiem saistībā ar personas piemērotību darbam paredzētajā amatā;

2) nodarbinātības laikā uzraugot darbinieka apzinīgumu un rīcību.

Piezīme. Par sodāmības neesību var pārliecināties, izmantojot sertifikātu, ko izdevusi dalībvalsts atbildīgā iestāde saskaņā ar Regulu (ES) 2016/1191. Ja tiek apsvērta iespēja pieņemt darbā darbiniekus no ārvalstīm, iepriekš minētās pārbaudes var veikt, pamatojoties uz līdzvērtīgiem sertifikātiem, ko izdevusi izcelsmes valsts, piemēram, pamatojoties uz “uzticamības sertifikātu”.

b) Turklāt personāla uzticamības noteikšanas procesā un kritērijos var būt jāapsver, vai:

1) informācijas sistēmas un dati, kam paredzēts nodrošināt piekļuvi, ir bijuši saistīti ar augstu drošuma seku smaguma pakāpi IS.I.OR.205. punktā noteiktajā riska novērtēšanas procesā;

2) riska analīzē identificēto riska kontroles vai mazināšanas pasākumu pamatā ir organizatoriskas/darbības procedūras (piemēram, informācijas tehnoloģiju pareiza konfigurēšana un administrēšana, datubāzes darbības, informācijas drošības uzraudzība utt.).

Šādos gadījumos attiecībā uz personālu, kam ir administratora tiesības vai neuzraudzīta un neierobežota piekļuve a) punkta 1) apakšpunktā minētajām sistēmām un datiem, vai attiecībā uz personālu, kas piemēro iepriekš b) punkta 2) apakšpunktā minētos pasākumus, var piemērot stingrākus kritērijus.

c) Izlūkdatus un jebkādu citu būtisku informāciju var iegūt, izskatot un analizējot publiskos avotus, piemēram, sociālos tīklus un tīmekļvietnes, ievērojot ierobežojumus, kas noteikti attiecīgajos valsts normatīvajos aktos.

d) Attiecībā uz dažām organizācijām, uz kurām attiecas *IS* daļa, var piemērot arī Regulu (ES) 2015/1998, kurā noteikts, ka darbiniekiem, kas ieņem noteiktus amatus, ir jāiztur iepriekšējās darbības pārbaudes, kā arī jāparedz mehānisms šo pārbaužu pastāvīgai pārskatīšanai. Šādos gadījumos organizācija var uzskatīt, ka darbinieku identitātes un uzticamības noskaidrošanai, kas ir noteikta *IS* daļā, saistībā ar viņu darba pienākumiem ir atbilstoši piemērot procesu un attiecīgos kritērijus, kas ir noteikti Regulā (ES) 2015/1998 attiecībā uz standarta un padziļinātām iepriekšējās darbības pārbaudēm. Tomēr jāatzīmē, ka atbilstība noteikumiem par identitātes un uzticamības noteikšanu atbilstoši *IS* daļai nenozīmē atbilstību noteikumiem par iepriekšējās darbības pārbaudēm, kas paredzēti Regulā (ES) 2015/1998.

## GM1 par IS.I.OR.245. punktu “Reģistrācija”

Dokumentācijas uzglabāšana ir nepieciešama, lai dokumentētu sasniegtos rezultātus vai sniegtu pierādījumus par veiktajām darbībām. Ieraksti kļūst par faktisku informāciju, kad tie ir reģistrēti, un tos nevar grozīt. Tāpēc dokumentiem nepiemēro versijas kontroli. Pat tad, ja attiecībā uz vienu un to pašu jautājumu tiek izveidots jauns ieraksts, iepriekšējais ieraksts paliek spēkā.

“Saņemtie apstiprinājumi”, kas ir minēti a) apakšpunkta 1) daļas i) punktā, ietver ikvienu “sertifikātu”, ko organizācija ir saņēmusi, ja to paredz organizācijas jomas īstenošanas noteikumi.

## AMC1 par IS.I.OR.245. punkta “Reģistrācija” a) apakšpunkta 1) daļas vi) punktu un a) apakšpunkta 5) daļu

Nodrošinot atbilstību a) apakšpunkta 1) daļas vi) punkta un a) apakšpunkta 5) daļas prasībām, organizācijai ir jāizstrādā datu glabāšanas politika, kurā ir noteiktas procedūras:

a) attiecīgo drošības datu datņu pārvaldībai;

b) to satura periodiskai novērtēšanai un

c) tādu kritēriju noteikšanai, kas ļauj dzēst ierakstus par informācijas drošības notikumiem, ja ir sasniegts a) apakšpunkta 5) daļas prasības mērķis.

## GM1 par IS.I.OR.245. punkta “Reģistrācija” a) apakšpunkta 1) daļas vi) punktu un a) apakšpunkta 5) daļu

Šā punkta a) apakšpunkta 1) daļas vi) punktā noteiktās prasības mērķis ir nodrošināt tādu informācijas drošības incidentu vai ievainojamību iespējamo pazīmju konstatēšanu, kas nav pamanāmas parastas darbības apstākļos (piemēram, iepriekš nezināmas situācijas), savukārt a) apakšpunkta 5) daļas prasības mērķis ir nodrošināt vajadzīgo elastību, lai kontrolētu saglabāto informācijas drošības notikumu apjomu.

Ieraksti par informācijas drošības notikumiem ietver notikumus, kas atzīti par tādiem, uz kuriem attiecas IS.I.OR.220. punkta a) apakšpunktā noteiktie atklāšanas pasākumi, kā arī citus informācijas drošības datus, kas iegūti no aktīviem, kuri ir noteikti atbilstoši IS.I.OR.205. punktam.

Datu glabāšanas politikā ir precizēts, kāda informācija un cik ilgi ir jāglabā vai jāarhivē. Daži norādījumi par datu glabāšanu ir sniegti *EUROCAE* dokumenta ED-206 2.6. nodaļā.

Kad datu kopas glabāšanas periods ir beidzies, to var dzēst vai pārvietot kā pastāvīgus vēsturiskos datus uz sekundāru vai terciāru krātuvi.

## AMC1 par IS.I.OR.245. punkta “Reģistrācija” c) un d) apakšpunktu

Nodrošinot atbilstību c) un d) apakšpunkta prasībām attiecībā uz visiem IS.I.OR.245. punkta a) un b) apakšpunktā noteiktajiem ierakstiem, organizācijai ir jāapsver šādi aspekti:

a) ieraksti ir jāuzglabā papīra vai elektroniskā formātā, vai abējādi. Vajadzības gadījumā ierakstiem jābūt pieejamiem pieņemamā laika posmā un jābūt izmantojamiem visā noteiktajā glabāšanas laikā. Glabāšanas laiks sākas, kad tiek izveidots dokuments;

b) ierakstu datu integritāte, pieejamība un autentiskums jāaizsargā saskaņā ar attiecīgo darbības datu aizsardzību, un tāpēc tiem ir jāietilpst IDPS tvērumā;

c) glabāšanas sistēmām ir jābūt aizsargātām pret nesankcionētu piekļuvi (t. i., pret personas datu nopludināšanas mēģinājumiem / ierakstu pārveidošanas mēģinājumiem), un tāpēc tajās jābūt ieviestiem informācijas drošības pasākumiem, kas īstenoti atbilstoši ar tiem saistītā informācijas drošības riska līmenim;

d) kad ieraksti vairs nav jāglabā, tie ir pienācīgi jāiznīcina un jāpārtrauc to glabāšanai izmantoto aktīvu ekspluatācija.

## GM1 par IS.I.OR.245. punkta “Reģistrācija” c) un d) apakšpunktu

**IERAKSTU PIEEJAMĪBA VISĀ GLABĀŠANAS PERIODĀ**

Ieteicams ievērot labo praksi attiecībā uz datu glabāšanu un attiecībā uz tādiem datiem, kas var būt jāatjauno, izmantot dublēšanas stratēģijas, piemēram, izmantot automatizētus dublēšanas rīkus, nošķirt vai ģeogrāfiski nodalīt rezerves kopiju glabāšanas vietas(-u), kā arī apsvērt dublēšanu bezsaistē, lai novērstu izspiedējvīrusu risku. Šāda prakse jāapsver arī tad, ja par reģistrāciju ir noslēgti līgumi ar pakalpojumu sniedzējiem, kuriem ir dalīti resursi.

Īpaša uzmanība jāpievērš būtiskām aparatūras un programmatūras izmaiņām, nodrošinot, ka saglabātie digitālie ieraksti joprojām ir pieejami un lasāmi (piemēram, datņu sistēma, lietotnes datnes formāts, nākotnē saderīgas datubāzu versijas utt.). Informācija papīra formātā ir jāarhivē atbilstošā vidē, kurā ieraksti ir aizsargāti pret nelabvēlīgu iedarbību (piemēram, pret pārmērīgu karstumu, gaismu vai mitrumu).

**IERAKSTU DATU INTEGRITĀTE UN AIZSARDZĪBA PRET NESANKCIONĒTU PIEKĻUVI**

Lai nodrošinātu autentiskuma un integritātes aizsardzību, parasti izmanto elektroniskos parakstus dokumentu līmenī. Elektroniskos parakstus var pievienot dokumenta datnei (piemēram, PDF datnei), lai nodrošinātu, ka ierakstu nav pārveidojis cits lietotājs, kas nav tā autors (integritāte), un ka autors ir tas, kurš tika paredzēts (autentiskums).

Turklāt, lai novērstu nesankcionētu piekļuvi, ierakstus var aizsargāt, piemēram, izmantojot ar darba pienākumiem pamatotu piekļuves kontroles (*RBAC*) pieeju, vai dažus ierakstus var aizsargāt ar paroli datņu līmenī. Komerciālajās lietotnēs ir iebūvētas paroles aizsardzības pamatfunkcijas to datņu formātiem. Piekļuves aizsardzību var arī nodrošināt, aizsargājot vidi, kurā tiek glabāti atsevišķie ieraksti (piemēram, piekļuves aizsardzība datubāzēm, koplietotajām datnēm, direktorijām utt.).

## GM1 par IS.I.OR.250. punkta “Informācijas drošības pārvaldības rokasgrāmata (IDPR)” a) apakšpunktu

Organizācija var arī izvēlēties daļu informācijas, kas noteikta IS.I.OR.250. punkta a) apakšpunktā, dokumentēt atsevišķos dokumentos (piemēram, procedūras). Šādā gadījumā tai ir jānodrošina, ka rokasgrāmatās ir iekļautas pienācīgas norādes par ikvienu atsevišķi glabāto dokumentu. Šādi dokumenti ir jāuzskata par organizācijas informācijas drošības pārvaldības sistēmas rokasgrāmatas neatņemamu daļu.

Ja struktūrai ir vairākas atļaujas vai deklarācijas, IDPR var būt piemērojama attiecībā uz vienu vai vairākām organizācijām vienlaikus, pamatojoties uz kopīgu IDPS. Šajā IDPR jāiekļauj vismaz katras organizācijas apstiprinājuma dokuments, un tas oficiāli jāapstiprina katras organizācijas atbildīgajam vadītājam vai atbildīgajai personai. Kopīgu atbildīgo personu var iecelt atbilstoši IS.I.OR.240. punkta d) apakšpunktam un norādījumiem, kas sniegti GM1 par IS.I.OR.240. punkta e) apakšpunktu.

Lai nodrošinātu, ka visas iesaistītās puses spēj pildīt savus pienākumus, visas rokasgrāmatas, procedūras un savstarpējo saziņu ieteicams sagatavot vienā valodā, piemēram, angļu valodā. Iesaistītās puses ietver kompetentās iestādes, ar kurām jāvienojas par šo vienoto valodu.

## AMC1 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas”

Neskarot izmaiņu paziņošanu, kas noteikta katrai organizācijai attiecīgajā īstenošanas regulā attiecībā uz jomām, kuras minētas Regulas (ES) 2023/203 2. panta 1. punktā, IS.I.OR.255. punkta a) apakšpunkta 1) daļā minētajā procedūrā tas, kā izmaiņas tiks pārvaldītas, ir jāierosina, ņemot vērā to būtiskumu. Jo īpaši jāpārbauda tās izmaiņas, kas varētu ietekmēt atbilstības *IS* daļas noteikumiem nodrošināšanu vai uzturēšanu vai kas varētu radīt nepieņemamu riska līmeni (piemēram, atbilstoši norādījumiem, kas sniegti GM1 par IS.I.OR.205. punkta c) apakšpunktu). Pēc šīs procedūras izveidošanas visas turpmākās izmaiņas tajā ir jāapstiprina kompetentajai iestādei.

Ja kompetentajai iestādei lūdz iepriekšēji apstiprināt izmaiņas, uz kurām neattiecas apstiprināta procedūra, vai ja šādas apstiprinātas procedūras nav, organizācijai jāsniedz vismaz šāda informācija:

* izmaiņu būtība un mērķis;
* izmaiņu ieviešanas plāns;
* izmaiņu verifikācijas plāns;
* izmaiņu iespējamā ietekme uz aviācijas drošumu.

Būtiska atkāpšanās no sākotnējā īstenošanas plāna izmaiņu procesā ir notikums, par kuru jāziņo kompetentajai iestādei, jo šīs atkāpšanās dēļ var būt jāpārskata izmaiņu ietekme.

## GM1 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas”

IS.I.OR.255. punkts ir strukturēts šādi:

ar šā punkta a) apakšpunktu tiek ieviesta iespēja organizācijai vienoties ar kompetento iestādi par to, ka izmaiņas IDPS var īstenot bez iepriekšēja apstiprinājuma, ja attiecībā uz šīm izmaiņām ir piemērojama izmaiņu procedūra;

ar šā punkta b) apakšpunktu tiek ieviests iepriekšējas apstiprināšanas (ko veic kompetentā iestāde) pienākums attiecībā uz izmaiņām, uz kurām neattiecas iepriekš minētā procedūra, un norādīts, kā šīs izmaiņas ir jāapstrādā.

Organizācijai jāapsver procedūras izveide, lai pārvaldītu izmaiņas un paziņotu par tām kompetentajai iestādei, kā paredzēts IS.I.OR.255. punkta a) apakšpunktā. Ja nav apstiprinātas procedūras, organizācijai attiecībā uz jebkurām izmaiņām būs jāpiesakās un jāsaņem apstiprinājums, kā noteikts IS.I.OR.255. punkta b) apakšpunktā. Jebkurā gadījumā kompetentā iestāde jāinformē par visām izmaiņām pēc to īstenošanas.

## GM2 par IS.I.OR.255. punktu “Informācijas drošības pārvaldības sistēmas izmaiņas”

**SAISTĪBA STARP IDPS IZMAIŅĀM UN NEPĀRTRAUKTU UZLABOŠANU**

Izmaiņas, kas izriet no organizācijas izveidotā nepārtrauktas uzlabošanas procesa (skat. IS.I.OR.260. punktu), jāapstrādā tāpat kā jebkuras citas izmaiņas atbilstoši norādījumiem, kas sniegti AMC1 par IS.I.OR.255. punktu un GM1 par IS.I.OR.255. punktu.

**PIEMĒRS IZMAIŅĀM, KAS VAR IETEKMĒT IDPS**

Turpmāk ir sniegti daži tādu izmaiņu piemēri, kas var ietekmēt IDPS vai kas var radīt nepieņemamu riska līmeni, un tādēļ kompetentajai iestādei tās ir jāpārbauda saskaņā ar IS.I.OR.255. punkta noteikumiem:

a) izmaiņas IDPS tvērumā, saskarnēs vai saistītajā politikā:

* organizācija paplašina savas darbības funkcijas un savā organizatoriskajā struktūrā integrē citu uzņēmumu;
* organizācija ir konstatējusi neatbilstību, kas liecina par nepareizu tvērumu;
* organizācija groza savu informācijas drošības politiku un/vai informācijas drošības mērķus, kas var ietekmēt aviācijas drošumu;
* izmaiņas organizācijas saskarnēs, kas rodas, piemēram, veicot izmaiņas iekšējās vai ārpakalpojumā nodotajās darbībās;

b) izmaiņas pienākumos un atbildībā, kā arī organizatoriskajā struktūrā, kas ietver šīs regulas ievērošanas īstenošanu un nepārtrauktu uzraudzību:

* atbildīgais vadītājs ir deleģējis personai vai personu grupai noteiktus pienākumus, kas ir paredzēti *IS* daļā;
* organizācija slēdz līgumus par informācijas drošības pārvaldības darbībām atbilstoši IS.I.OR.235. punktam;

c) izmaiņas riska pārvaldībai izmantotajā metodoloģijā:

* organizācija maina varbūtības vai ietekmes klasifikāciju riska pārvaldības metodoloģijā, piemēram, lai iegūtu lielāku detalizācijas pakāpi;
* organizācija ievieš izmaiņas savā riska risināšanas metodoloģijā;
* organizācija integrē savu informācijas drošības riska pārvaldību pašreizējās pārvaldības sistēmās;

d) izmaiņas drošības notikuma pārvaldības procesā:

* organizācija nolemj slēgt līgumus par drošības notikuma pārvaldības darbībām;
* organizācija maina procesu, kā tiek paziņots par drošības notikumiem, un kritērijus ātrāka risinājuma panākšanai augstākā vadības līmenī;
* organizācija maina savu ievainojamību mazināšanas politiku;
* organizācija maina savu incidentu seku novēršanas procedūru.

**PIEMĒRS IZMAIŅĀM, KAS NEIETEKMĒ IDPS**

Ne visas ar informācijas drošību saistītās darbības izmaiņas ietekmē IDPS, tāpēc ne par visām izmaiņām ir jāziņo kompetentajai iestādei saskaņā ar IS.I.OR.255. punkta noteikumiem. Šādas izmaiņas var raksturot šādi scenāriji:

* pēc veiksmīgi atklāta drošības notikuma, kas ļoti iespējams varēja kļūt par incidentu, organizācija nolemj īstenot plašu informatīvi izglītojošu kampaņu par kiberdrošību visiem darbiniekiem;
* personāla mācību programmas un/vai mācību satura atjaunināšana organizācijā, kas izriet no ieviestajiem nepārtrauktas uzlabošanas procesiem;
* organizācija aizstāj programmatūras rīku, ko tā izmanto sensitīvu datņu šifrēšanai, ar citu programmatūras risinājumu;
* organizācija ir nolēmusi veikt iekšēju pārstrukturēšanu ar darbību saistītu iemeslu dēļ, mainot departamentu vai nodaļu nosaukumus, bet nemainot pienākumus un atbildību (piemēram, atbildīgais vadītājs), kas saistīti ar organizācijas IDPS;
* organizācija nolemj atjaunināt pašreizējo preventīvo kontroli, piemēram, konfigurējot jaunu ugunsmūri savā iekšējā tīklā.

## AMC1 par IS.I.OR.260. punktu “Pastāvīgi uzlabojumi”

Pastāvīgu uzlabojumu procesa (*CIP*) mērķim, kā noteikts IS.I.OR.200. punkta b) apakšpunktā, jābūt pastāvīgai IDPS rezultativitātes, piemērotības un atbilstības uzlabošanai. Tas jāpanāk, profilaktiski un sistemātiski novērtējot IDPS un visus tās elementus, tostarp tās gatavību. Novērtējumā jāņem vērā citu informācijas drošības un nodrošināšanas procesu rezultāti un secinājumi, tostarp revīziju, vadības pārskatu, darbības rādītāju, rezultativitātes un gatavības izvērtējums, kā arī atvasināto korektīvo pasākumu un labojumu rezultāti.

Jāveic vismaz šādas darbības:

a) uzlabošanas iespēju noteikšana, pamatojoties uz IDPS piemērotības, rezultativitātes, atbilstības un, ja nepieciešams, efektivitātes novērtējuma rezultātiem, kā arī pamatojoties uz jebkādiem citiem uzlabojumu ierosinājumiem. Novērtējumā jāizskata darbības rādītāji, kas atspoguļo tās procesus un elementus, un noteiktos rezultativitātes un gatavības mērķus;

b) apzināto iespēju izvērtēšana attiecībā uz izmaksām un ieguvumiem, nevēlamas ietekmes neesību vai samazināšanu un noteikto mērķu un paredzēto rezultātu sasniegšanu;

c) ierosinājums vadībai par izvērtētajām uzlabošanas iespējām un ieteikumi par darbībām, kas palīdzētu tai pārskatīšanas un lēmumu pieņemšanas procesā;

d) saskaņā ar lēmumu, kas pieņemts atbilstoši c) apakšpunktam, darbību un izmaiņu plānošana, izstrāde un īstenošana attiecībā uz IDPS, tās procesiem vai elementiem, lai panāktu uzlabojumus;

e) īstenoto darbību un IDPS izmaiņu rezultativitātes izvērtēšana, un vajadzības gadījumā pārbaude par to, vai konstatēto nepilnību pamatcēlonis ir novērsts.

Vadībai jānovērtē un jāizskata pastāvīgu uzlabojumu procesu rezultāti plānotos laika posmos, lai nodrošinātu pastāvīgu IDPS rezultativitāti, atbilstību un piemērotību, lemtu par prioritāšu noteikšanu darbību un izmaiņu īstenošanai, kā arī pārskatītu vai noteiktu jaunus mērķus vai uzdevumus nolūkā nodrošināt pastāvīgus uzlabojumus.

## GM1 par IS.I.OR.260. punktu “Pastāvīgi uzlabojumi”

IS.I.OR.260. punkts ietver nodrošināšanas procesus attiecībā uz IDPS tādā veidā, ko var uzskatīt par līdzvērtīgu drošuma nodrošināšanai atbilstīgi *ICAO* dokumentam Nr. 9859 “Drošības pārvaldības rokasgrāmata (*SMM*)”, kurā izklāstīta darbības rādītāju uzraudzība un mērīšana, DPS izmaiņu pārvaldība un pastāvīga uzlabošana.

Šajā regulā:

* IS.I.OR.260. punkta a) apakšpunkts attiecas uz IDPS rezultativitātes un gatavības novērtēšanu, izmantojot atbilstīgus darbības rādītājus;
* IS.I.OR.260. punkta b) apakšpunkts attiecas uz saskaņā ar IS.I.OR.260. punkta a) apakšpunktu konstatēto nepilnību uzlabošanas pasākumiem, t. i., attiecīgiem labojumiem un korektīviem pasākumiem un uz pastāvīgu uzlabojumu procesu.

Līdzīgi noteikumi par pastāvīgiem uzlabojumiem ir paredzēti citās informācijas pārvaldības sistēmās, piemēram, ISO/IEC 27001 (skat. šā dokumenta II papildinājumu).

Organizāciju konteksts un riska vide pastāvīgi mainās, tāpēc ir nepieciešama organizācijas mērķu, arhitektūras, organizatorisko struktūru un procesu dinamiska pielāgošana, izstrāde un maiņa, lai uzturētu informācijas drošības riskus pieņemamā līmenī. Tāpēc IDPS ir jāuzskata par organizācijas daļu/elementu, kas pastāvīgi mainās un tiek pilnveidots un kas ir pastāvīgi jāuzrauga un jāuzlabo, lai nodrošinātu atbilstību organizācijas drošuma mērķiem un rezultativitātei.

Pastāvīgu uzlabojumu procesa mērķis ir pastāvīgi uzlabot IDPS rezultativitāti, piemērotību, pietiekamību un, ja tas tiek uzskatīts par nepieciešamu, efektivitāti. Organizācija var integrēt *IS* daļas pastāvīgu uzlabojumu procesu kādā citā jau izmantotā pastāvīgu uzlabojumu procesā un var izmantot tādas metodes kā “Plānot, darīt, pārbaudīt, rīkoties” (*PDCA*) ciklu vai “Noteikt, mērīt, analizēt, uzlabot, kontrolēt” (*DMAIC*) (skat. arī GM1 par IS.I.OR.200. punktu).

Pastāvīgu uzlabojumu procesa pamatā ir preventīvs un sistemātisks IDPS un visu tās elementu novērtējums, tostarp IDPS nodrošināto informācijas drošības procesu un kontroles pasākumu, novērtējums. Novērtējums jāveic, ņemot vērā organizatoriskos mērķus attiecībā uz vēlamo darbības rādītāju, rezultativitātes un gatavības līmeni. Šie mērķi var būt noteikti nolūkā ne tikai nodrošināt atbilstību šajā regulā noteiktajām prasībām, bet arī ietvert tos mērķus, kas ir noteikti organizācijas politikā vai standartos un vadības lēmumos.

Iepriekšminētā novērtējuma pamatā ir darbības rādītāju izvērtējumu, revīziju, riska un incidentu procesu rezultāti, kā arī iepriekš piemērotie korektīvie pasākumi un labojumi. Daži faktori, kas jāņem vērā, veicot novērtējumu, ir šādi:

* **piemērotība** attiecas uz sistēmas spēju noteikt disciplīnas, kas nepieciešamas informācijas drošības pārvaldībai, piemēram, pienācīgi izmantojot vispārpieņemtus nozares standartus attiecībā uz atbilstības nodrošināšanu šīs regulas prasībām;
* **IDPS rezultativitāti** un IDPS vadīto procesu un kontroles pasākumu efektīvu īstenošanu novērtē, analizējot, vai:
* informācijas drošības riski tiek pārvaldīti, lai sasniegtu drošuma mērķus;
* ir sasniegti vēlamie IDPS rezultāti, ir izpildītas prasības vai mērķi;
* tiek pārvaldītas visu veidu nepilnības, tostarp prasības vai kontroles pasākuma neievērošana vai nepareiza īstenošana;
* IDPS **efektivitāte** attiecas uz vienkāršotu procedūru ieviešanu, tomēr lietderības uzlabojumi nedrīkst nelabvēlīgi ietekmēt rezultativitāti.

**Uzlabošanas iespēju noteikšana**

Uzlabošanas iespējas var noteikt, pamatojoties uz pastāvīgu uzlabojumu procesa novērtējuma rezultātiem, vai arī tās var ieviest kā ierosinājumus no citiem avotiem. Šajā noteikšanā bieži tiek ietvertas atkāpes vai korektīvi pasākumi, kā arī neefektīvi procesi vai kontroles pasākumi, kas netiek koriģēti.

Uzlabojumu ierosinājumi tiek sagatavoti, pamatojoties uz šādiem avotiem:

* riska pārvaldība – regulāras riska analīzes un turpmākās riska risināšanas rezultāti ir galvenais faktors IDPS uzlabošanā, kur riska risināšanas process ietver īstenoto drošības pasākumu uzraudzību un to rezultativitātes novērtēšanu;
* darbības rādītāju un rezultativitātes izvērtējums – secinājumi no (galvenajiem) darbības rādītājiem, to mērījumiem, analīzes un nepārtrauktas uzraudzības, kā arī rezultativitātes novērtējuma rezultāti, tostarp vēlāk piemēroto labojumu un korektīvo pasākumu rezultāti;
* gatavības izvērtējums, tostarp turpmāko labojumu un korektīvo pasākumu rezultāti;
* pieredze, kas gūta no drošības incidentu atklāšanas, apstrādes un reaģēšanas procesa un iespējamā pamatcēloņa novēršanas;
* (iekšējo) revīziju rezultātus var izmantot, lai pārbaudītu, vai IDPS un kontroles pasākumi, kas ietilpst revīzijas tvērumā, atbilst organizācijas prasībām, un noteiktu to, kurās jomās ir iespējami uzlabojumi;
* pašreizējā rīcības plāna pārskatīšana un izvērtēšana, nosakot vai pārskatot mērķus vai lēmumu par uzlabošanas iespējām un darbībām;
* organizācijas ieteikumu programma (uzlabojumu ieteikumi), pārskati, apsekojumi vai novērtējumi ar darbiniekiem, vai atgriezeniskā saite no piegādātājiem vai saskarpusēm.

Visi šā procesa rezultāti ir jādokumentē. Izrietošās darbības var integrēt vispārējā rīcības plānā, kas ir centralizēti saskaņots un periodiski pārskatīts saskaņā ar attiecīgo politiku. Izveidoto rīcības plānu var sīkāk iedalīt taktiskā īstermiņa / vidēja termiņa rīcības plānā un stratēģiskā ilgtermiņa rīcības plānā.

## AMC1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” a) apakšpunktu

a) **IDPS REZULTATIVITĀTES IZVĒRTĒJUMS**

Nodrošinot atbilstību IS.I.OR.260. punkta a) apakšpunktam, organizācijai jābūt ieviestam procesam savas IDPS rezultativitātes uzraudzīšanai, mērīšanai, izvērtēšanai un pārbaudīšanai, ar kuru nosaka to:

1) kas uzrauga, mēra, analizē un izvērtē rezultātus, un pieņem atbildīgus lēmumus;

2) kad ir jāveic iepriekš minētās darbības;

3) kuras uzraudzības, mērīšanas, analīzes un izvērtēšanas metodes tiek izmantotas, lai nodrošinātu salīdzināmus un reproducējamus rezultātus.

Novērtējumu kalendārajam plānojumam jābūt samērīgam ar maksimālo riska līmeni, kas noteikts atbilstoši IS.I.OR.205. punktam.

AMC1 par IS.I.OR.260. punkta a) apakšpunktu minētajā organizācijas IDPS rezultativitātes uzraudzības, mērīšanas, izvērtēšanas un pārskatīšanas procesā jāiekļauj vismaz šādi elementi:

1) datu par darbību rādītājiem vākšana un glabāšana, kā arī papildu informācija, kas var būt noderīga uzraudzībai;

2) rādītāju analīze, lai noteiktu tendences un atkāpes no iepriekš noteiktiem darbības mērķiem.

b) **IDPS GATAVĪBAS NOVĒRTĒJUMS**

Organizācijai jānovērtē savas IDPS gatavība, izmantojot piemērotu gatavības modeli, lai noteiktu jomas, kurās nepieciešami IDPS uzlabojumi. Lai to izdarītu, organizācijai:

1) jānosaka vai jāpieņem gatavības modelis, kas satur svarīgus un būtiskus procesus un spējas, ko paredzēts īstenot un uzturēt;

2) attiecībā uz katru novērtēto procesu vai spēju jānodrošina, ka modelī ir noteikti kritēriji, pēc kuriem, nosakot gatavības līmeni, jānovērtē un jāizvērtē konkrēti aspekti, īpašības un rezultativitāte;

3) jānosaka vēlamais gatavības mērķa līmenis katram novērtētajam procesam vai spējai.

c) Attiecībā uz katru gatavības modelī iekļauto novērtēto informācijas drošības procesu vai spēju organizācijai:

1) jāizvērtē un jāpamato pašreizējais gatavības līmenis;

2) jānosaka visas jomas, kurās jāveic uzlabojumi, lai sasniegtu vēlamo gatavības līmeni;

3) jāvāc un jāreģistrē pierādījumi par ieviestās IDPS stiprajām un vājajām pusēm un tās izvērtēto gatavību.

## GM1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” a) apakšpunktu

a) Kopumā jāuzrauga, jāmēra un jāizvērtē vismaz šādi IDPS elementi:

1) riska novērtēšanas un risināšanas process (tostarp riski saskarnēs ar citām organizācijām);

2) neatbilstību un korektīvo pasākumu pārvaldība;

3) incidentu un ievainojamību pārvaldība;

4) personāla kompetenču pārvaldība.

b) Pašreizējie gatavības modeļi IDPS gatavības izvērtēšanai

Kopumā, lai noteiktu vai pieņemtu gatavības modeli (*MM*), var apsvērt šādus modeļus:

* kiberdrošības spēju gatavības modelis (C2M2), 1.1. versija. ASV Enerģētikas departaments publicēja šo modeli 2014. gadā. Ar to ievieš gatavības rādītāju līmeņus (*MIL*) diapazonā no 0 līdz 3, un tajā aplūko ne tikai darbības rādītāju līmeņus, bet arī darbības praksi (sadaļā par pieejas mērķiem un pieejas virzību), kā arī nodrošināšanas praksi (sadaļā par pārvaldības mērķiem un institucionalizācijas virzību);
* sistēmas drošības inženierijas – spējas gatavības modelis (*SSE-CMM*), ko 2008. gadā publicēja ISO kā standartu ISO 21827. Tajā galvenā uzmanība pievērsta inženierijas praksei un ievērojami mazākā mērā darbības praksei, kas iedalīta 11 drošības pamatpaņēmienos un 11 projektu un darbības pamatpaņēmienos. Tajā ir ieviests piecu spēju līmeņu kopums diapazonā no “īstenotas neoficiāli” līdz “pastāvīgi uzlabojošās”;
* *NIST* kiberdrošības sistēma (*NIST CSF*), 1.1. versija, ko *NIST* publicēja 2018. gada aprīlī. Lai gan tā nav piedāvāta kā gatavības modelis, šajā sistēmā ir noteikti četri “īstenošanas līmeņi”– no “daļējs” līdz “adaptīvs”, kas ir kvalitatīvs organizatoriskās kiberdrošības riska pārvaldības prakses mērs. Tajā galvenā uzmanība ir pievērsta kiberdrošības riska pārvaldības funkcionalitātei un atkārtojamībai;
* *ATM* kiberdrošības gatavības modelis, 1. izdevums, ko publicējis *EUROCONTROL NM* 2019. gada februārī *ATM* jomā ietilpstošajām organizācijām. Lai gan tas nav paredzēts plašākam lietojumam, to var pielāgot pēc vajadzības. Tajā noteikti pieci gatavības līmeņi – no “nepastāvošs” līdz “adaptīvs”, iedvesmojoties no *NIST CSF* “līmeņu” terminoloģijas. Faktiski šā modeļa pamatā ir *NIST CSF* kopā ar dažiem ISO/IEC 27001 elementiem.

Turpmāk 1. tabulā iepriekš minētie gatavības modeļi ir pielīdzināti teorētiskam piecu līmeņu gatavības modelim.

**1. tabula. Pašreizējo gatavības modeļu atbilstība teorētiskam piecu līmeņu gatavības modelim**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Atbilstība piecu līmeņu gatavības modelim** | **C2M2** | ***Eurocontrol NM*** | **ISO 21827** | ***NIST CSF* 1.1** |
| **Sākotnējs** | MIL 0 | Nepastāvošs | Īstenots neoficiāli |  |
| **Noteikts** | MIL 1 (Sākotnējs) | Daļējs | Plānots un izsekots | Daļējs |
| **Ieviests** | MIL 2 (Identificēts) | Noteikts | Pienācīgi noteikts | Balstīts riska izvērtējumā |
| **Pārvaldīts** | MIL 3 (Pārvaldīts) | Apstiprināts | Kvantitatīvi kontrolēts | Atkārtojams |
| **Uzlabots** |  | Adaptīvs | Tiek pastāvīgi uzlabots | Adaptīvs |

Neviens konkrēts gatavības līmenis nav nepieciešams. Ja tomēr tiek panākta atbilstība, organizācijas noteiks, kuras modeļu prasības jau ir izpildītas (obligāti), un var izvēlēties sasniegt organizācijai izdevīgu līmeni (brīvprātīgi). Ilgtermiņā augstāku gatavības līmeņu sasniegšana var paaugstināt pārraudzības iestāžu uzticēšanos, un tas var ietekmēt attiecībā uz šādu organizāciju veikto pārraudzības pasākumu līmeni.

## AMC1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” b) apakšpunktu

Ja ir konstatēta nepilnība, organizācijai savlaicīgi jāreaģē, ievērojot noteiktu procesu, kura rezultātā nepilnība, ar to saistītās sekas tiek pārvaldītas un, ja nepieciešams, tiek novērsta tās turpmāka atkārtošanās vai parādīšanās citviet.

Pamatojoties uz nepilnības ietekmes un apjoma izvērtējumu un iespējamo ietekmi uz IDPS, procesā ir jāietver šādi atbilstības kritēriji:

a) bez nepamatotas kavēšanās tiek lemts par labojumiem un to īstenošanu, lai ierobežotu nepilnības ietekmi un risinātu tās sekas, kā arī lai attiecīgā gadījumā to kontrolētu vai likvidētu;

b) tiek lemts par to, vai ir vajadzīgi un jāīsteno korektīvi pasākumi, lai novērstu nepilnības cēloni(-ņus) un veicinošos faktorus, pamatojoties uz pamatcēloņu analīzi un to darbību izvērtējumu, ar kurām novērš cēloni un kuru mērķis ir nodrošināt samērīgumu ar nepilnības radītajām sekām un ietekmi;

c) tiek pārbaudīts, vai īstenotās darbības:

1) ir efektīvas un rada pieņemamus nenovērstos riskus;

2) nerada neparedzētu blakusiedarbību, kas radītu citas nepilnības, jaunus riskus vai IDPS neatbilstību piemērojamām prasībām, kā arī

3) attiecībā uz korektīvajiem pasākumiem – vai tie efektīvi mazina vai likvidē pamatcēloni;

d) par konstatētajām nepilnībām, rīcības plānu un veiktajām darbībām tiek ziņots organizācijas atbildīgajam vadītājam vai deleģētajai(-ām) personai(-ām) un vajadzības gadījumā citiem iesaistītajiem vai skartajiem darbiniekiem un pusēm un tie tiek pārskatīti kopā ar minētajām pusēm;

e) konstatētās nepilnības, plānotās un īstenotās korekcijas un/vai korektīvie pasākumi tiek dokumentēti kā pierādījumi, norādot termiņus un atbildīgās personas, vadības sniegto atgriezenisko saiti, iepriekš c) apakšpunktā minētā procesa posma rezultātus un, ja nepieciešams, pieņemtos lēmumus par izmaiņām IDPS.

## GM1 par IS.I.OR.260. punkta “Pastāvīgi uzlabojumi” b) apakšpunktu

“Vajadzīgie uzlabošanas pasākumi”, kas ir minēti IS.I.OR.260. punkta b) apakšpunktā, ir labojumi vai korektīvi pasākumi, ko veic, lai novērstu nepilnības, vai darbības, kuru mērķis ir uzlabot IDPS rezultativitāti un gatavību.

Procesam, kas atbilst AMC1 par IS.I.OR.260. punktu noteiktajiem kritērijiem, jāietver šādi aspekti:

a) nepilnību apmēra, ietekmes, konteksta un ierosinātāju noteikšana, izvērtējot tos atbilstoši atsevišķiem noteiktiem kritērijiem, analizējot iespējamo ietekmi uz IDPS, tostarp iespējamo pastāvēšanu citās jomās;

b) lemšana par labojumiem un to īstenošanu, lai nekavējoties ierobežotu nepilnības ietekmi un risinātu tās sekas un lai attiecīgā gadījumā kontrolētu vai likvidētu to;

c) lemšana par korektīviem pasākumiem, kas vajadzīgi, lai novērstu nepilnības (pamat)cēloni(-ņus), un kas ir samērīgi ar sekām;

d) to IDPS elementu atkārtota novērtēšana, ko var ietekmēt īstenotās darbības, lai nodrošinātu, ka netiek radīts papildu risks;

e) AMC1 par IS.I.OR.260. punkta b) apakšpunktu c) punktā minēto īstenoto darbību pārbaude;

f) ziņošana vadībai par procesa posmu rezultātiem un to izskatīšana kopā ar vadību (skat. AMC1 par IS.I.OR.260. punkta b) apakšpunktu);

g) iepriekš minēto procesa posmu rezultātu dokumentēšana un apliecināšana ar pierādījumiem (skat. AMC1 par IS.I.OR.260. punkta b) apakšpunktu e) punktu).

## I papildinājums

## Piemēri apdraudējumu scenārijiem, kam var būt nelabvēlīga ietekme uz drošumu

Turpmāk sniegts neizsmeļošs saraksts ar tādu informācijas drošības apdraudējumu scenāriju piemēriem, kas var nelabvēlīgi ietekmēt drošumu un ko var apsvērt iestādes un organizācijas.

**1. piemērs. Lidaparāta un *ATC* digitālie sakari**

* **Apdraudējuma vektora aktīvi/joma**
* *ATC* balss un zemes automatizācijas sistēmas
* Zemes sakaru nodrošinātāji
* Gaiss-zeme/zeme-gaiss RF sakaru pakalpojumu sniedzēji
* Lidaparāti un aktīvi, ko izmanto balss un datu pārraides posma sakariem
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): sistēmas darbības rādītāju pārsniegšana, sakaru kanāla piesātināšana
* Apdraudējums (integritāte): pārtvērējuzbrukumi vai ievadītājuzbrukumi
* Apdraudējums (konfidencialitāte): pasīva sakaru noklausīšanās, spiegošana aparatūras ierīcē
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Pakalpojumu traucējumi liedz *ATC* saziņu ar vienu vai vairākiem lidaparātiem un/vai *ATC* zemes sistēmu
* Manipulācijas ar datiem, izmantojot pārtvērējuzbrukumu, sniegtu pilotam un/vai *ATC* sistēmai nepatiesu informāciju, kas varētu radīt drošuma apdraudējumu vai datu iepludināšanu lidaparāta vai zemes sistēmās, lai radītu pakalpojumu un spēju traucējumus
* Nav īpašu reglamentējošu prasību attiecībā uz datu vai balss šifrēšanu datu pārraides posma sakariem; tomēr konfidencialitātes nolūkā aktīvi, ko izmanto pakalpojumu nodrošināšanai un sniegšanai, ir jākontrolē un jāizmanto tikai tie resursi, kuriem nepieciešama piekļuve, lai nodrošinātu, ka pakalpojumus nekādi nevar traucēt un ka ar tiem nevar manipulēt

**2. piemērs. Falsificēti gaisa satiksmes dati**

* **Apdraudējuma vektora aktīvi/joma**
* Interneta pakalpojumu sniedzējs (*ISP*)
* *ATM* pakalpojumu tīkls(-i)
* Novērošanas dati
* *ATC* sistēmas
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* *ISP* kompromitējums (konfidencialitāte): uzbrucējs iegūst nesankcionētu piekļuvi *ISP* sistēmām vai infrastruktūrai, kas nodrošina tīkla pakalpojumus *ATM* sistēmai
* Datu falsificēšana (integritāte): kad *ISP* ir kompromitēts, uzbrucējs var manipulēt ar datiem to pārsūtīšanas laikā Tas var ietvert nepatiesu datu iepludināšanu vai patiesu datu dzēšanu/pārveidošanu
* Pakalpojuma atteikums (pieejamība): uzbrucējs var arī pilnīgi pārtraukt datu pārraidi, tādējādi izraisot pakalpojuma atteikumu (*DoS*) *ATM* sistēmai
* Ļaunatūras iepludināšana (integritāte/pieejamība): uzbrucējs var izmantot kompromitēto *ISP* kā platformu ļaunatūras iepludināšanai sistēmās, lai radītu turpmākus traucējumus vai nodrošinātu iespēju veikt papildu uzbrukumus
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* *ISP* kompromitējums: sensitīvu datu pārtveršana un/vai manipulēšana ar tiem, kas ietekmē drošu gaisa satiksmes vadību
* Datu falsifikācija: nepareiza situācijas apzināšanās, kuras dēļ var samazināties distance starp lidaparātiem, un nepareizi gaisa satiksmes kontroles lēmumi
* Pakalpojuma atteikums: pasliktinās *ATC* spēja nodrošināt distancēšanu, tāpēc tiek aktivizētas ārkārtas procedūras, tostarp samazināta spēja, un, iespējams, tiek slēgtas lielas gaisa telpas zonas

**3. piemērs. Lidaparāta ekspluatantu, lidotspējas uzturēšanas vadības organizāciju (*CAMO*) un lidaparāta tehniskās apkopes organizāciju programmatūras piegādes ķēde un zemes infrastruktūra, tostarp aprīkojums, ko izmanto lidaparātu pārvaldības, ekspluatācijas un tehniskās apkopes atbalstam**

* **Apdraudējuma vektora aktīvi/joma**
* Lidaparātu ekspluatantu, *CAMO* un tehniskās apkopes organizāciju piegādes ķēde
* Lidaparāta ekspluatanta vai tehniskās apkopes iekšējā zemes infrastruktūra, ko izmanto, lai pārvaldītu lidaparātu un ekspluatāciju (aparatūra/programmatūra), un citi informācijas tehnoloģiju aktīvi
* Informācijas tehnoloģiju aktīvi, ko izmanto, lai atjauninātu lidaparāta sistēmas (programmatūru un aparatūru), kuras izmanto tehniskās apkopes darbībām
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): aparatūras/programmatūras/sistēmas darbības traucējumi
* Apdraudējums (integritāte): kompromitēta aparatūra/programmatūra/sistēma
* Apdraudējums (konfidencialitāte): kompromitēta aparatūra/programmatūra/sistēma
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Meteoroloģiskās informācijas izplatīšanas traucējumi lidaparāta lidojuma laikā var mazināt lidaparāta apkalpes spēju izvairīties no iespējami bīstamiem meteoroloģiskajiem apstākļiem (piemēram, no spēcīgām vētrām / miglas naktī)
* Manipulācija ar navigācijas datiem/datubāzi samazinās uzticēšanos lidojuma plāniem un navigācijas displejiem
* Kontroles trūkums un nepietiekama piekļuve informācijai par flotes tehniskās apkopes programmu vai lidojuma apkalpes plānošanu ietekmē organizāciju spēju nodrošināt drošu ekspluatāciju

**Tauriņveida analīzes piemērošana šim piemēram**

Tā kā galīgā interese ir tikai par sekām aviācijas drošumam, tiek apvienotas divas saskaņotas dažādu riska dimensiju tauriņveida analīzes.

| **Informācijas drošības tauriņveida analīzes elements** | **Aviācijas drošuma tauriņveida analīzes elements** |
| --- | --- |
| **Informācijas drošības apdraudējums**1) Aparatūras/programmatūras ievainojamības izmantošana: traucēta sistēmas funkcija.2) Aparatūras/programmatūras ievainojamības izmantošana: kompromitēta sistēmas integritāte.3) Aparatūras/programmatūras ievainojamības izmantošana: ar kompromitētu(-ām) sistēmu(-ām) apstrādātas informācijas konfidencialitāte. |  |
| **Informācijas drošības preventīvās barjeras** |  |
| **Informācijas drošības apdraudējums un galvenie notikumi**1) Traucēta sistēmas funkcionalitāte (apdraudējums) →traucēta/neuzticama sistēmas funkcionalitāte.2) Kompromitēta sistēmas integritāte (apdraudējums) →sistēmas funkcionēšana ir neparedzama.3) Izpaužama informācija (apdraudējums) →neatklājama informācijas eksfiltrācija. | Drošuma apdraudējums:1) traucēta/neuzticama sistēmas funkcionalitāte;2) sistēmas funkcionēšana ir neparedzama;3) neatklājama informācijas eksfiltrācija. |
| **Mazinošās informācijas drošības barjeras** | Preventīvās drošuma barjeras:1) piekļuves kontroles līdzekļu izmantošana sistēmas administrēšanā;2) u. c. |
| **Ietekme uz informācijas drošību**1) Sistēmas funkcijas zudums (= nedarbojas ražošanas sistēma).2) Sistēmas funkcijas integritātes zudums (= atsevišķas sistēmas funkcijas darbojas nepareizi / nedarbojas).3) Informācijas konfidencialitātes zudums (= var noplūst noteikta informācija). | Drošuma apdraudējums un galvenie notikumi:1) sistēmas funkcijas zudums (apdraudējums) *→ operatīvajā tehniskās apkopes sistēmā*;2) sistēmas funkcionālās integritātes zudums (apdraudējums) → *sistēmas darbojas ar nepareizu informāciju*;3) informācijas konfidencialitātes zudums (apdraudējums) *→**konfidenciālas tehniskās apkopes un lidaparāta iekšējās informācijas noplūde.* |
|  | Mazinošās drošuma barjeras:1) rezerves procedūru izmantošana, lai novērstu nepareizas tehniskās apkopes darbības;2) procedūru izmantošana, lai nodrošinātu lidaparāta programmatūras integritāti. |
|  | Sekas drošumam:1) kļūdainas tehniskās apkopes darbības;2) nepareizi izpildītas tehniskās apkopes darbības;3) informācijas eksfiltrācija ļauj noteikt ievainojamības;4) lidaparātu sistēmu traucējums, neparedzama sistēmas darbība, galveno lidaparātu sistēmu (piemēram, dzinēja kontrole) zaudējums. |

**4. piemērs. Projektēšanas un ražošanas uzņēmumu programmatūra, piegādes ķēde, projektēšanas un ražošanas zemes infrastruktūra**

* **Apdraudējuma vektora aktīvi/joma**
* Projektēšanas un ražošanas uzņēmumu detaļu, aparatūras un programmatūras piegādes ķēde
* Projektēšanas un ražošanas uzņēmumu iekšējā zemes infrastruktūra, ko izmanto, lai pārvaldītu programmatūru/aparatūru, kuru izmanto tādu produktu ražošanā un izstrādāšanā, ko lietos lidaparātu ražotāji, ekspluatanti vai *ATM*/*ANS* zemes automatizācijas sistēmu (aparatūra/programmatūra) informācijas tehnoloģiju aktīvi
* Projektēšanas un ražošanas uzņēmumu informācijas tehnoloģiju aktīvi, ko izmanto to klienti, lai atjauninātu sistēmas lidaparātā (programmatūra/aparatūra), kuras lieto tehniskās apkopes darbībās vai *ATM*/*ANS* zemes automatizācijas sistēmās
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): *DoS* uzbrukumu rezultātā sistēmas, ko izmanto, lai uzglabātu, pārraidītu informāciju un apmainītos ar to, tiek padarītas nepieejamas būtiskām darbībām
* Apdraudējums (integritāte): sistēmas, ko izmanto, lai uzglabātu, pārraidītu informāciju un apmainītos ar to, tiek kompromitētas, izmantojot pārtvērējuzbrukumus
* Apdraudējums (konfidencialitāte): sistēmas, ko izmanto, lai uzglabātu, pārraidītu informāciju un apmainītos ar to, tiek pakļautas iekšējam vai ārējam apdraudējumam
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Tādu sistēmu darbības traucējumi, ko izmanto, lai uzglabātu, pārraidītu informāciju un apmainītos ar to tādā veidā, kas liegtu lidaparāta un tā sistēmu pareizu pārvaldību un nelabvēlīgi ietekmētu lidaparāta darbību
* Sistēmas, ko izmanto informācijas glabāšanai, pārraidīšanai un apmaiņai, vairs nevar uzskatīt par uzticamām. Ja tās netiek uzturētas tādā līmenī, lai nodrošinātu, ka visu informācijas apmaiņu, datus un programmatūru var uzskatīt par uzticamu, tiek traucēta gan darbība uz zemes, gan lidaparāta ekspluatācija
* Nekontrolēta piekļuve sistēmām, ko izmanto informācijas (tostarp tādas informācijas, kas tiek saņemta un apmainīta ar piegādes ķēdi) glabāšanai, pārraidīšanai un apmaiņai, var ļaut piekļūt tehniskai informācijai, ko varētu izmantot, lai izstrādātu sarežģītākus uzbrukumus, kas vērsti pret drošumam kritiski svarīgām sistēmām

**5. piemērs. Mācību sistēma**

* **Apdraudējuma vektora aktīvi/joma**
* Piegādes ķēde, ar kuru nodrošina visu programmatūru un aparatūru, kas tiks izmantota mācību sistēmās vai mācību ierīcēs (tostarp lidojumu trenažieros), kuras izmanto pilota vai *ATM*/*ANS* zemes sistēmu personāla mācībās
* Iekšējā infrastruktūra, ko izmanto visā programmatūrā un aparatūrā, kura tiks izmantota tādu produktu (aparatūras vai programmatūras) projektēšanā, ražošanā vai izgatavošanā, kas tiks izmantoti lidaparātā vai *ATM*/*ANS* zemes sistēmās
* Visu to programmatūras un aparatūras iekšējo darbības jomu un sistēmas pārvaldība, kas tiks izmantotas tādu produktu (aparatūras vai programmatūras) projektēšanā, ražošanā vai izgatavošanā, kurus lietos lidaparātos vai *ATM/ANS* zemes sistēmās
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): izmantojot *DoS* uzbrukumus, mācību sistēmas vai mācību ierīces tiek padarītas nepieejamas, kad tās ir nepieciešams izmantot
* Apdraudējums (integritāte): mācību sistēmas vai mācību ierīces ir kompromitētas, izmantojot pārtvērējuzbrukumus
* Apdraudējums (konfidencialitāte): funkcionāliem modeļiem, informācijai un datiem, kas iegulti mācību sistēmās vai mācību ierīcēs, piekļūst iekšējs vai ārējs apdraudējums
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Mācību sistēmu (aparatūras un programmatūras) traucējums ietekmēs organizāciju spēju uzturēt personāla kvalifikāciju. Tas arī liegtu lidaparātu un tā sistēmu pienācīgu ekspluatāciju un ietekmētu *ATM*/*ANS* zemes sistēmu tehniskās apkopes darbības
* Mācību modelis vai atteices režīmi un ar tiem saistītie ārkārtas apstākļi atšķiras no reālās aviācijas sistēmas darbības un tādēļ izraisa neatbilstošu reakciju. Ja mācību sistēmas nav uzticamas, tas ietekmēs organizāciju spēju nodrošināt pietiekami kvalificētu personālu to darbībām (piloti, tehniskās apkopes personāls vai *ATM*/*ANS* personāls uz zemes, kas nav saņēmis atbilstošas mācības, ir jāpārkvalificē)
* Mācību sistēmu kontroles un pieejamības trūkums ietekmē organizāciju spēju uzturēt mācību sistēmu, par kuru ir zināms, ka tā ir uzticama. Turklāt nekontrolēta piekļuve mācību sistēmām, kurās ir iegulti funkcionāli modeļi, informācija un dati, var ļaut iegūt tehnisku informāciju, ko var izmantot sarežģītākiem uzbrukumiem pašai mācību sistēmai vai reālai sistēmai, kura ir kritiski svarīga drošumam

**6. piemērs. Lidostas degvielas piegādes sistēma un saistītā infrastruktūra**

* **Apdraudējuma vektora aktīvi/joma**
* Degvielas uzglabāšanas un sadales infrastruktūra uz zemes
* Digitālās sistēmas degvielas sūknēšanas un mērīšanas kontrolei
* Degvielas piegādes ķēde, tostarp trešo pušu degvielas piegādātāji
* Lidostu informācijas tehnoloģiju aktīvi, ko izmanto degvielas krājumu pārvaldībai un piegāžu plānošanai
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): degvielas apgādes vai piegādes sistēmu darbības traucējumi
* Apdraudējums (integritāte): iejaukšanās degvielas kontroles sistēmu vai mērierīču darbībā
* Apdraudējums (konfidencialitāte): nesankcionēta piekļuve degvielas apgādes un piegādes datiem
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Degvielas piegādes traucējumi var izraisīt lidojumu kavēšanos vai atcelšanu, radot darbības traucējumus un iespējamas drošuma problēmas, ja degvielas rezerves kļūst kritiski mazas
* Iejaukšanās degvielas kontroles sistēmu vai mērierīču darbībā var izraisīt nepareiza degvielas daudzuma piegādi lidaparātam, kas var ietekmēt lidaparāta svara un balansēšanas aprēķinus un radīt degvielas izbeigšanās incidentus
* Nesankcionēta piekļuve degvielas apgādes datiem varētu sniegt iespēju apdraudējuma radītājiem manipulēt ar degvielas plānošanas vai krājumu datiem, tādējādi radot traucējumus lidostas darbībā un apgrūtinot degvielas pieejamību lidaparātiem

**7. piemērs. Valsts kompetentās iestādes *NOTAM* sistēma un saistītā infrastruktūra**

* **Apdraudējuma vektora aktīvi/joma**
* Valsts *NOTAM* sistēmas infrastruktūra un digitālā saskarne
* Piegādes ķēde *NOTAM* sistēmas uzturēšanai un atjaunināšanai
* Valsts kompetentās iestādes IT aktīvi, ko izmanto *NOTAM* izveidei, izplatīšanai un glabāšanai
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): *NOTAM* sistēmas darbības pārtraukums vai nepieejamība
* Apdraudējums (integritāte): *NOTAM* datu falsifikācija vai nesankcionēta *NOTAM* izveide
* Apdraudējums (konfidencialitāte): nesankcionēta piekļuve *NOTAM* datiem
* **Apdraudējumu scenāriju un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* Traucējumi *NOTAM* sistēmā var kavēt būtiskas aeronavigācijas informācijas izplatīšanu pilotiem un gaisa satiksmes vadības dispečeriem, tādējādi, iespējams, radot iespējamas drošuma problēmas
* *NOTAM* datu falsifikācijas vai nesankcionētas *NOTAM* izveides dēļ var tikt izplatīta nepareiza informācija un piloti lēmumu pieņemšanai var izmantot nepatiesus vai maldinošus datus
* Nesankcionēta piekļuve *NOTAM* datiem var izraisīt informācijas noplūdi, potenciāli atklājot sensitīvu operatīvo informāciju

**8. piemērs. Aeronavigācijas iestādes lidotspējas direktīvas (*AD*) sistēma un saistītā infrastruktūra**

* **Apdraudējuma vektora aktīvi/joma**
* *EASA* *AD* sistēmas infrastruktūra un digitālā saskarne
* Piegādes ķēde *AD* sistēmas uzturēšanai un atjaunināšanai
* *EASA* IT aktīvi, ko izmanto *AD* izveidei, izplatīšanai un glabāšanai
* **Neizsmeļošs iespējamo apdraudējumu apkopojums**
* Apdraudējums (pieejamība): *AD* sistēmas darbības pārtraukums vai nepieejamība
* Apdraudējums (integritāte): *AD* datu falsifikācija vai nesankcionēta *AD* izveide
* Apdraudējums (konfidencialitāte): nesankcionēta piekļuve *AD* datiem
* **Apdraudējumu un to iespējamās nelabvēlīgās ietekmes uz drošumu apkopojums**
* *AD* sistēmas darbības traucējumi var liegt būtiskas lidojumderīguma informācijas izplatīšanu pilotiem un gaisa satiksmes vadības dispečeriem, iespējams, radot drošuma problēmas
* *AD* datu falsifikācijas vai neatļautas *AD* izveides dēļ var tikt izplatīta nepareiza informācija, un lidaparātu ekspluatanti un tehniskās apkopes organizācijas lēmumu pieņemšanai var izmantot nepatiesus vai maldinošus datus
* Nesankcionēta piekļuve *AD* datiem var izraisīt informācijas noplūdi, potenciāli atklājot sensitīvu operatīvo informāciju

## II papildinājums

## Galvenie uzdevumi, kas izriet no *IS* daļas ieviešanas, tostarp atbilstība *NIST CSF*

## 1.1. versijas kompetencēm un ISO/IEC 27001 punktiem un kontroles pasākumiem

| ***IS* daļas galvenais uzdevums** | **Pasākuma veids** | **Atsauce** |
| --- | --- | --- |
| **Pārvaldības pasākums, darbības pasākums** | ***IS* daļa** | ***NIST CSF* 1.1. versija** | **ISO/IEC 27001** |
| **Funkcija** | **Kategorija** | **Rindkopa Punkts** | **A pielikums. Kontrole** |
| **:2013** | **:2013** |
| Izveidot un ekspluatēt informācijas drošības pārvaldības sistēmu (IDPS) | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkts | IDENTIFICĒT | ID.RM | 4.6.1.1. |  |  |
| Noteikt IDPS tvērumu atbilstoši *IS* daļas prasībām | Pārvaldības pasākums | IS.I.OR.205. punkta a) apakšpunkts | IDENTIFICĒT | ID.BE-2ID.BE-4ID.AM-5 | 4.3. |  |  |
| Ieviest un uzturēt informācijas drošības politiku | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 1. punkts | IDENTIFICĒT | ID.GV-1 | 5.2. | A5.1. | A5.1. |
| Identificēt un izskatīt informācijas drošības riskus | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 2. punktsIS.I.OR.205. punkts | IDENTIFICĒT | ID.GV-4ID.RA | 6.1.2.8.1.8.2. |  |  |
| Īstenot informācijas drošības riska risināšanas pasākumus | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 3. punktsIS.I.OR.210. punkts | AIZSARGĀT | PR.PT | 6.1.3.8.1.8.3. |  |  |
| Īstenot pasākumus, lai atklātu informācijas drošības notikumus un identificētu tos, kas ir saistīti ar aviācijas drošumu | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 5. punktsIS.I.OR.220. punkts | ATKLĀT | DE.AE-3DE.CM-1DE.CM-2DE.CM-3 |  | A11.1.2.A12.4.1.A12.4.3.A16.1.7. | A7.2.A8.15.A5.28. |
| Īstenot pasākumus, par kuriem ir paziņojusi kompetentā iestāde | Darbības pasākums | IS.I.OR.200. punkta a) apakšpunkta 6. punkts |  |  | 10.1. | A6.1.3. | A5.5. |
| Veikt atbilstīgas korektīvas darbības, lai novērstu kompetentās iestādes paziņotos konstatējumus (neatbilstības) | Abi | IS.I.OR.200. punkta a) apakšpunkta 7. punktsIS.I.OR.225. punkts |  |  | 10.1. | A6.1.3. | A5.5. |
| Īstenot ārējās informācijas drošības pārskatu sniegšanas shēmu | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 8. punktsIS.I.OR.230. punkts | REAĢĒT | RS.CO-2RS.CO-3RS.CO-4RS.CO-5 | 7.4. | A6.1.3.A16.1.2.A16.1.3. | A5.5.A6.8. |
| Uzraudzīt atbilstību šai regulai un ziņot par konstatējumiem augstākajai vadībai | Darbības pasākums | IS.I.OR.200. punkta a) apakšpunkta 12) daļa | IDENTIFICĒT | ID.GV-3 | 9.2. | A18.2.1.A18.2.2. | A5.35.A5.36. |
| Aizsargāt informācijas, ar kuru apmainās, konfidencialitāti | Darbības pasākums | IS.I.OR.200. punkta a) apakšpunkta 13. punkts | AIZSARGĀT | PR.DS-1PR.DS-2 |  | A8.2.2.A13.2. | A5.13.A5.14. |
| Īstenot un uzturēt pastāvīgu uzlabojumu procesu, lai noteiktu IDPS rezultativitāti un gatavību un censtos to uzlabot | Pārvaldības pasākums | IS.I.OR.200. punkta b) apakšpunktsIS.I.OR.260. punkts | IDENTIFICĒT | ID.RA-6ID.SC-4 | 4.4.9.1.9.3.10.1.10.2. | A5.1.2.A16.1.7.A17.1.3.A18.2.1. | A5.1.A5.28.A5.29.A5.35. |
| AIZSARGĀT | PR.IP-7PR.IP-10 |
| ATKLĀT | DE.DP-5 |
| REAĢĒT | RS.MI-3RS.IM-2 |
| NOVĒRST SEKAS | RC.IM-2 |
| Dokumentēt un uzturēt visus galvenos procesus, procedūras, funkcijas un pienākumus | Pārvaldības pasākums | IS.I.OR.200. punkta c) apakšpunkts | IDENTIFICĒT | ID.AM-6ID.GV-4ID.RM-1ID.SC-1ID.SC-2 | 4.2.5.2.5.3. | A5.1.A6.1.1. | A5.1.A5.2. |
| AIZSARGĀT | PR.AT-2PR.AT-4PR.AT-5PR.IP-12 |
| ATKLĀT | DE.DP-1 |
| REAĢĒT | RS.CO-1RS.AN-5 |
| Identificēt visus elementus, kas varētu būt pakļauti informācijas drošības riskiem | Pārvaldības pasākums | IS.I.OR.205. punkta a) apakšpunkts | IDENTIFICĒT | ID.AM-1ID.AM-2ID.AM-4ID.AM-5 | 4.3. | A8.1.1. | A5.9. |
| Identificēt saskarnes ar citām organizācijām, kas varētu radīt informācijas drošības riskus | Pārvaldības pasākums | IS.I.OR.205. punkta b) apakšpunkts | IDENTIFICĒT | ID.BE-1ID.BE-2ID.BE-4ID.BE-5 | 4.3. |  |  |
| Identificēt informācijas drošības riskus un piešķirt riska līmeni | Pārvaldības pasākums | IS.I.OR.205. punkta c) apakšpunkts | IDENTIFICĒT | ID.RA-1ID.RA-2ID.RA-3ID.RA-4ID.RA-5 | 6.1.2. |  |  |
| Pārskatīt un atjaunināt riska novērtējumu, pamatojoties uz noteiktiem kritērijiem | Darbības pasākums | IS.I.OR.205. punkta d) apakšpunkts | IDENTIFICĒT | ID.RM | 8.2. |  | A5.7. |
| Regulas (ES) 2017/373 III pielikuma C apakšiedaļā (ATM/ANS.OR daļa) minētās organizācijas kopīgi veic drošības atbalsta novērtējumu | Darbības pasākums | IS.I.OR.205. e) apakšpunkts |  |  |  |  |  |
| Izstrādāt un īstenot pasākumus risku novēršanai un pārbaudīt to rezultativitāti | Darbības pasākums | IS.I.OR.210. punkta a) apakšpunkts | AIZSARGĀT | PR.IPPR.PT | 6.1.3.8.3. |  |  |
| Paziņot riska novērtējuma rezultātus vadībai, citam personālam un citām organizācijām, kam ir kopīga saskarne | Darbības pasākums | IS.I.OR.210. punkta b) apakšpunkts | IDENTIFICĒT | ID.AM-3ID.BE-1ID.BE-2ID.BE-4ID.RM-3ID.SC-3 | 8.1. |  |  |
| AIZSARGĀT | PR.IP-7 |
| Izveidot iekšējās informācijas drošības ziņošanas sistēmu, kas ļautu apkopot informācijas drošības notikumus no personāla un izvērtēt tos | Pārvaldības pasākums | IS.I.OR.200. punkta a) apakšpunkta 4. punktsIS.I.OR.215. punkta a) apakšpunktsIS.I.OR.215. e) apakšpunkts | IDENTIFICĒT | ID.AM-3 | 7.4. | A16.1.1.A16.1.2. | A5.28.A6.8. |
| Nodrošināt, ka nolīgtās organizācijas ziņo par informācijas drošības notikumiem | Pārvaldības pasākums | IS.I.OR.215. punkta c) apakšpunkts | REAĢĒT | RS.CO-2RS.CO-4 | 7.4. | A15.1.1.A16.1.2. | A5.19.A6.8. |
| Analizēt iekšēji paziņotos atgadījumus, lai identificētu informācijas drošības notikumus, incidentus un ievainojamības | Darbības pasākums | IS.I.OR.215. punkta b) apakšpunkta 1) daļa – b) apakšpunkta 3) daļa | IDENTIFICĒT | ID.RA-1 |  | A12.6.1., A16.1.1., A16.1.4. | A8.8.A5.24.A5.25. |
| ATKLĀT | DE.AE-2DE.AE-3DE.AE-5 |
| Īstenot pasākumus, lai procesos un darbībās atklātu informācijas drošības notikumus, kas var potenciāli ietekmēt aviācijas drošumu | Darbības pasākums | IS.I.OR.220. punkta a) apakšpunkts | ATKLĀT | DE.AEDE.CMDE.DP |  | A11.1.2.A12.4.1.A12.6.1.A16.1.1.A16.1.2.A16.1.3.A16.1.4.A16.1.5. | A7.2.A8.8.A8.15.A8.16.A5.24.A5.25.A5.26.A6.8. |
| AIZSARGĀT | PR.PT-1 |
| Īstenot pasākumus, lai reaģētu uz informācijas drošības notikumiem, kas var izraisīt informācijas drošības incidentu | Darbības pasākums | IS.I.OR.220. punkta b) apakšpunkts | REAĢĒT | RS.RPRS.ANRS.MI |  | A16.1.5. | A5.26. |
| Sadarboties izmeklēšanā ar citām organizācijām, kas uzlabo tās darbību informācijas drošību | Pārvaldības pasākums | IS.I.OR.215. punkta d) apakšpunkts | REAĢĒT | RS.AN-3RS.AN-5 |  | A15.1.2.A15.1.3.A16.1.7. | A5.20.A5.21.A5.28. |
| Īstenot pasākumus, lai novērstu informācijas drošības incidentu sekas | Darbības pasākums | IS.I.OR.220. punkta c) apakšpunkts | NOVĒRST SEKAS | RC.RP-1RC.IM-1 |  | A16.1.5.A16.1.6. | A5.26.A5.27. |
| Pārvaldīt riskus, kas ir saistīti ar nolīgtajām darbībām attiecībā uz informācijas drošības pārvaldību | Pārvaldības pasākums | IS.I.OR.235. punkts | IDENTIFICĒT | ID.SC-1ID.SC-2 |  | A15.1.A15.2. | A5.19.A5.20.A5.21.A5.22. |
| Izveidot un uzturēt procesu, lai nodrošinātu, ka ir pietiekami daudz darbinieku visu ar informācijas drošības pārvaldību saistīto pasākumu īstenošanai | Pārvaldības pasākums | IS.I.OR.240. punkta f) apakšpunkts | IDENTIFICĒT | ID.AM-5ID.AM-6ID.GV-2 | 7.1. | A6.1.1. | A5.2. |
| Izveidot un uzturēt procesu, lai nodrošinātu, ka darbiniekiem ir vajadzīgā kompetence ar informācijas drošības pārvaldību saistīto darbību veikšanai | Pārvaldības pasākums | IS.I.OR.240. punkta g) apakšpunkts | IDENTIFICĒT | ID.AM-5ID.AM-6 | 7.2. | A7.2.2. | A6.3. |
| AIZSARGĀT | PR.AT-1 |
| Izveidot un uzturēt procesu, lai nodrošinātu, ka darbinieki atzīst ar piešķirtajām funkcijām un uzdevumiem saistītos pienākumus | Pārvaldības pasākums | IS.I.OR.240. punkta h) apakšpunkts | IDENTIFICĒT | ID.GV-2ID.GV-3 | 7.3.7.4. | A7.1.2. | A6.2. |
| Pārbaudīt to darbinieku identitāti un uzticamību, kam ir piekļuve informācijas sistēmām | Pārvaldības pasākums | IS.I.OR.240. punkta i) apakšpunkts | AIZSARGĀT | PR.AC-6PR.IP-11 | 7.1. | A7.1.1. | A6.1. |
| Arhivēt, aizsargāt un glabāt ierakstus un nodrošināt, ka tie ir izsekojami noteiktu laiku | Darbības pasākums | IS.I.OR.245. punkts | IDENTIFICĒT | ID.RA-4 | 7.5. | A8.2.2.A8.2.3.A11.1.3.A11.1.4.A12.1.3.A12.3.1.A12.4.1.A12.4.2.A12.4.3. | A5.10.A5.13.A7.3.A7.5.A8.6.A8.10.A8.13.A8.15. |
| AIZSARGĀT | PR.AC-2PR.AC-3PR.AC-4PR.DS-1PR.DS-4PR.DS-5PR.DS-6PR.IP-4PR.IP-6PR.PT-1 |
| Labot konstatēto neatbilstību pēc kompetentās iestādes paziņojuma termiņā, par kuru ir panākta vienošanās ar kompetento iestādi | Darbības pasākums | IS.I.OR.225. punkts |  |  | 10.1. | A18.1.1.A18.2. | A5.31.A5.35.A5.36. |
| Īstenot informācijas drošības ziņošanas sistēmu saskaņā ar Regulu (ES) Nr. 376/2014 | Pārvaldības pasākums | IS.I.OR.230. punkta a) apakšpunkts |  |  |  |  |  |
| Paziņot kompetentajai iestādei un ar zināmiem nosacījumiem arī citām personām par informācijas drošības incidentiem vai ievainojamību | Darbības pasākums | IS.I.OR.230. punkta b) apakšpunktsIS.I.OR.230. punkta c) apakšpunkts | ATKLĀT | DE.DP-3 | 7.4. | A16.1.1.A16.1.2.A16.1.3. | A5.24.A6.8. |
| REAĢĒT | RS.CO-2RS.CO-3RS.CO-4RS.CO-5 |
| NOVĒRST SEKAS | RC.CO-3 |
| Regulāri novērtēt IDPS rezultativitāti un gatavību | Darbības pasākums | IS.I.OR.260. punkta a) apakšpunkts |  |  | 9. | A5.1.2.A12.7.1.A16.1.6. | A5.1.A5.27.A8.34. |
| Vajadzības gadījumā veikt pasākumus IDPS uzlabošanai.Atkārtoti novērtēt IDPS elementus, kurus ietekmē īstenotie pasākumi | Darbības pasākums | IS.I.OR.260. punkta b) apakšpunkts |  |  | 10. | A5.1.2. | A5.1. |
| Nodrošināt kompetentās iestādes pieejamību nolīgtajai organizācijai | Pārvaldības pasākums | IS.I.OR.235. punkta b) apakšpunkts |  |  | 9.3. | A6.1.3.A15.1.A15.2. | A5.5.A5.20.A5.22. |
| Augstākā vadība nodrošina, ka ir pieejami visi nepieciešamie resursi, lai izpildītu regulas prasības | Pārvaldības pasākums | IS.I.OR.240. punkta a) apakšpunkta 1. punkts | IDENTIFICĒT | ID.AM-5ID.AM-6 | 7.1. | A6.1.1. | A5.2. |
| Augstākā vadība izveido informācijas drošības politiku, informē par to un demonstrē pamatizpratni par Regulu | Pārvaldības pasākums | IS.I.OR.240. panta a) apakšpunkta 2) daļa un a) apakšpunkta 3) daļa | IDENTIFICĒT | ID.GV-1 | 5.1.5.2.7.4. | A5.1.1.A7.2.1.A7.2.2. | A5.1.A5.4.A6.3. |
| AIZSARGĀT | PR.AT-1PR.AT-4 |
| Iecelt atbildīgo personu vai personu grupu ar atbilstošām zināšanām, lai pārvaldītu Regulas prasību izpildi | Pārvaldības pasākums | IS.I.OR.240. punkta b) apakšpunktsIS.I.OR.240. punkta c) apakšpunktsIS.I.OR.240. punkta d) apakšpunkts | IDENTIFICĒT | ID.AM-6ID.GV-2 | 7.1.7.2. | A6.1.1.A7.2.1.A7.2.2. | A5.2.A5.4.A6.3. |
| AIZSARGĀT | PR.AT-1PR.AT-4 |
| Izveidot un uzturēt informācijas drošības pārvaldības rokasgrāmatu (IDPR) | Pārvaldības pasākums | IS.I.OR.250. punkts |  |  | 7.5.1. | A6.1.3.A12.1.1. | A5.5.A5.37. |
| Izstrādāt procedūru, kā informēt kompetento iestādi par IDPS izmaiņām | Pārvaldības pasākums | IS.I.OR.255. punkta a) apakšpunkts | IDENTIFICĒT | ID.AM-3 | 7.4.7.5.1. | A6.1.3.A13.2.1.A13.2.2. | A5.5.A5.14. |
| Pārvaldīt IDPS izmaiņas un informēt kompetento iestādi un/vai pieprasīt izmaiņu apstiprināšanu | Pārvaldības pasākums | IS.I.OR.255. punkta a) apakšpunktsIS.I.OR.255. punkta b) apakšpunkts | IDENTIFICĒT | ID.AM-3 | 7.4. | A6.1.3.A13.2.1.A13.2.2. | A5.5.A5.14. |

## III papildinājums

## Aviācijas pakalpojumu piemēri

Turpmāk sniegts neizsmeļošs un nepilnīgs tādu aviācijas pakalpojumu uzskaitījums, ko var izmantot par pamatu tam, lai noteiktu organizācijas riska novērtējuma tvērumu.

|  |
| --- |
| Aeronavigācijas digitālās kartēšanas pakalpojums |
| *AIM* (ārējā) |
| Apakšreģionu *DCB* vienotā pakalpojuma sniegšana |
| Apakšreģionu/valsts *ASM* |
| Apakšreģionu/vietējā *ATFCM* |
| *APP ACC* |
| Ar *ATM-MET* nesaistītu pakalpojumu sniedzējs |
| Ar aviāciju nesaistīti lietotāji (ārējie) |
| *ATC* (ārējā) |
| *ATM* |
| *ATM-MET* pakalpojuma sniedzējs |
| Augstākas pakāpes *ATC* |
| Civilo gaisa telpas izmantotāju darbību centrs |
| *ER ACC* |
| *FIS*/*TIS* datu integrators |
| Laikatskaite (ārējā) |
| Lidlauka *ATM-MET* pakalpojuma sniedzējs |
| Lidlauka zonas vadības tornis (*TWR*) |
| Lidosta |
| Navigācijas infrastruktūra – satelīta |
| Navigācijas infrastruktūra – zemes |
| Novērošanas infrastruktūra lidostā |
| Novērošanas infrastruktūra maršrutā |
| Novērošanas infrastruktūra *TMA* |
| Reģionālā *AIM* |
| Reģionālā *ASM* |
| Reģionālā *ATFCM* |
| Sakaru infrastruktūra |
| Statisko aeronavigācijas datu pakalpojums |
| Valsts *AIM* |
| Valsts gaisa telpas izmantotāju darbību centrs |

1. Šā izdevuma spēkā stāšanās datumu lūdzam skatīt *ED* Lēmumā 2023/009/R, kas publicēts *EASA* oficiālajā publikācijā. [↑](#footnote-ref-2)