URDHËR
Nr. 85, datë 25.3.2026

PËR MIRATIMIN E RREGULLOREVE PËR PËRCAKTIMIN E RREGULLAVE PËR ZBATIMIN E VENDIMIT TË KËSHILLIT TË MINISTRAVE NR. 1095, DATË 24.12.2020, "PËR MIRATIMIN E KËRKESAVE THELBËSORE NË FUSHËN E AVIACIONIT CIVIL", TË NDRYSHUAR, NË LIDHJE ME MENAXHIMIN E RREZIQEVE TË SIGURISË SË INFORMACIONIT ME NJË NDIKIM TË MUNDSHËM NË SIGURINË NË OPERIM[1]

Në zbatim të pikës 4, neni 102, të Kushtetutës; të pikës 2, shkronjës "ç", neni 7, të nenit 11 dhe nenit 108, të ligjit nr. 96/2020, "Kodi Ajror i Republikës së Shqipërisë"; të pikës 3.1(b), shtojca II, të pikës 3.3(b) dhe pikës 5(b), shtojca IV, të pikës 8.1(c), shtojca V, të pikës 2.1.1 dhe pikës 5.2, shtojca VII, të pikës 5.1(c) dhe pikës 5.4(b), shtojca VIII, të vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, "Për miratimin e kërkesave thelbësore në fushën e aviacionit civil", të ndryshuar; si dhe në përputhje me ligjin nr. 9658, datë 18.12.2006, "Për ratifikimin e marrëveshjes shumëpalëshe ndërmjet Komunitetit Evropian dhe shteteve anëtare të tij, Republikës së Shqipërisë, Bosnjës dhe të Hercegovinës, Republikës së Bullgarisë, Republikës së Kroacisë, Republikës së Maqedonisë, Republikës së Islandës, Republikës së Malit të Zi, Mbretërisë së Norvegjisë, Republikës së Rumanisë, Republikës së Serbisë dhe Misionit Administrativ të Përkohshëm të Kombeve të Bashkuara në Kosovë, për krijimin e një zone të përbashkët të aviacionit evropian",

URDHËROJ:

---

[1] Ky urdhër përafron pjesërisht Rregulloren e Komisionit (BE) nr. **2022/1645** e datës 14 korrik 2022 që përcakton rregullat për zbatimin e rregullores (BE) 2018/1139 të Parlamentit Evropian dhe të Këshillit, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm mbi sigurinë në operim për organizatat e mbuluara nga Rregulloret e Komisionit (BE) nr. 748/2012 dhe (BE) nr. 139/2014 dhe që ndryshon Rregulloret e Komisionit (BE) nr. 748/2012 dhe (BE) nr. 139/2014, botuar në Fletoren Zyrtare të BE-së nr. *L 248, 26.9.2022,* plotësisht rregulloren zbatuese të Komisionit (BE) **2025/22** e 19 dhjetorit 2024, që ndryshon rregulloren e deleguar (BE) nr. 2022/1645, për sa u takon kërkesave për sigurinë e informacionit të organizatave, që ofrojnë shërbime në tokë, botuar në Fletoren Zyrtare të BE-së nr. *L 2025/22, 7.3.2025, pjesërisht* rregulloren e Komisionit (BE) nr. **2023/203**, e datës 27 tetor 2022, për përcaktimin e rregullave për zbatimin e rregullores (BE) 2018/1139 të Parlamentit Evropian dhe të Këshillit, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë e aviacionit për organizatat e mbuluara nga Rregulloret e Komisionit (BE) nr. 1321/2014, (BE) nr. 965/2012, (BE) nr. 1178/2011, (BE) 2015/340, Rregulloret Implementuese të Komisionit (BE) 2017/373 dhe (BE) 2021/664, dhe për autoritetet kompetente të mbuluara nga Rregulloret e Komisionit (BE) nr. 748/2012, (BE) nr. /2012, (BE) nr. 1178/2011, (BE) 2015/340 dhe (BE) nr. 139/2014, Rregulloret Zbatuese të Komisionit (BE) 2017/373 dhe (BE) 2021/664 dhe që ndryshon rregulloret e komisionit (BE) nr. 1178/2011, (BE) nr. 748/2012, (BE) nr. 965/2012, (BE) nr. 139/2014, (BE) nr. 1321/2014, (BE) 2015/340, dhe Rregulloret Zbatuese të Komisionit (BE) 2017/373 dhe (BE) 2021/664, botuar në Fletoren Zyrtare të BE-së nr. L 31, 2.2.2023, pjesërisht rregulloren (BE) **2024/1109**, botuar në Fletoren Zyrtare të BE-së nr. L, 2024/1109, 23.5.2024, pjesërisht rregulloren zbatuese të Komisionit (BE) **2023/1769**, të datës 12 shtator 2023 që përcakton kërkesat teknike dhe procedurat administrative për miratimin e organizatave të përfshira në projektimin ose prodhimin e sistemeve dhe përbërësve të menaxhimit të trafikut ajror/shërbimeve të lundrimit ajror dhe që ndryshon rregulloren zbatuese (BE) 2023 /203, botuar në FZ të BE-së L228, 15.9.2023, Rregulloren Zbatuese e Komisionit (BE) **2025/2293**, e datës 10 nëntor 2025, që ndryshon rregulloren zbatuese (BE) 2023/203, në lidhje me kërkesat e zbatueshme për organizatat që i nënshtrohen një deklarate dhe korrigjon rregulloret (BE) nr. 1178/2011, (BE) nr. 748/2012, (BE) nr. 965/2012, (BE) nr. 139/2014, (BE) nr. 1321/2014, (BE) 2015/340 dhe rregulloren zbatuese (BE) 2017/373.

1. Miratimin e rregullores “Për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, ‘Për miratimin e kërkesave thelbësore në fushën e aviacionit civil”, i ndryshuar në lidhje me menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhri nr. 57, datë 13.3.2024, dhe urdhri nr. 170, datë 13.9.2022’, i ndryshuar”, sipas shtojcës I që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.

2. Miratimin e rregullores “Për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, ‘Për miratimin e kërkesave thelbësore në fushën e aviacionit civil’, i ndryshuar” në lidhje me menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhrat nr. 79, datë 15.4.2024, nr. 80, datë 30.6.2023, i ndryshuar; nr. 178, datë 20.12.2023, i ndryshuar; nr. 171, datë 11.11.2025; nr. 193, datë 6.10.2022, i ndryshuar; nr. 119, datë 29.9.2023, dhe për autoritetet kompetente të mbuluara nga urdhrat nr. 57, datë 13.3.2024; nr. 79, datë 15.4.2024; nr. 80, datë 30.6.2023, i ndryshuar; nr. 178, datë 20.12.2023, i ndryshuar; nr. 171, datë 11.11.2025; nr. 170, datë 13.9.2022, i ndryshuar; nr. 193, datë 6.10.2022, i ndryshuar; nr. 119, datë 29.9.2023”, sipas shtojcës II që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.

3. Ngarkohet Autoritetit i Aviacionit Civil për ndjekjen dhe për zbatimin e këtij urdhri.

Ky urdhër hyn në fuqi menjëherë dhe botohet në Fletoren Zyrtare.

MINISTËR I INFRASTRUKTURËS DHE ENERGJISË
Enea Karakaçi

SHTOJCA I
RREGULLORE PËR PËRCAKTIMIN E RREGULLAVE PËR ZBATIMIN E VENDIMIT TË KËSHILLIT TË MINISTRAVE NR. 1095, DATË 24.12.2020, “PËR MIRATIMIN E KËRKESAVE THELBËSORE NË FUSHËN E AVIACIONIT CIVIL”, I NDRYSHUAR, NË LIDHJE ME KËRKESAT PËR MENAXHIMIN E RREZIQEVE TË SIGURISË SË INFORMACIONIT ME NJË NDIKIM TË MUNDSHËM NË SIGURINË NË OPERIM PËR ORGANIZATAT E MBULUARA NGA URDHRI I MINISTRIT NR. 57, DATË 13.3.2024, DHE URDHRI I MINISTRIT NR. 170, DATË 13.9.2022, I NDRYSHUAR

Neni 1
Qëllimi

Kjo rregullore përcakton kërkesat që duhen përmbushur nga organizatat e përmendura në nenin 2 për të identifikuar dhe menaxhuar rreziqet e sigurisë së informacionit me ndikim të mundshëm në sigurinë në operim, të cilat mund të ndikojnë në sistemet e teknologjisë së informacionit dhe komunikimit dhe të dhënat e përdorura, për qëllime të aviacionit civil dhe për të zbuluar ngjarjet e sigurisë së informacionit, si dhe për të identifikuar ato që konsiderohen si incidente të sigurisë së informacionit me ndikim të mundshëm në sigurinë në operim dhe për t’iu përgjigjur atyre incidenteve të sigurisë së informacionit dhe për t’u rikuperuar nga ato.

Neni 2
Fusha e zbatimit

1. Kjo Rregullore zbatohet për organizatat e mëposhtme:

a) organizatat e prodhimit dhe organizatat e projektimit që u nënshtrohen nënpjesëve G dhe J të seksionit A të aneksit I (pjesa 21) të urdhrit të ministrit nr. 57, datë 13.3.2024, "Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesat e aftësisë së organizatave të projektimit dhe prodhimit", me përjashtim të organizatave të projektimit dhe prodhimit që janë të përfshira vetëm në projektimin dhe/ose prodhimin e avionëve ELA2, siç përcaktohet në nenin 1(2), shkronja "j" e urdhrit të ministrit nr. 57, datë 13.3.2024, "Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor, ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesat e aftësisë së organizatave të projektimit dhe prodhimit";

b) Operatorët e aerodromit dhe ofruesit e shërbimeve të menaxhimit të vendqëndrimit që i nënshtrohen aneksit III "Kërkesat për organizatën (pjesa-ADR.OR)" të urdhrit të ministrit nr. 170, datë 13.9.2022, "Për miratimin e rregullores për përcaktimin e kërkesave dhe procedurave administrative, që lidhen me aerodromet në Republikën e Shqipërisë", të ndryshuar.

c) Organizatat e përpunimit në tokë që i nënshtrohen Rregullores që përcakton kërkesat për ofrimin e sigurt të shërbimeve të përpunimit në tokë dhe për organizatat që i ofrojnë ato, që përafron rregulloren e deleguar të Komisionit (BE) 2025/20, që:

i. për të ofruar shërbimet përkatëse, duhet të mbledhin, ruajnë, analizojnë ose përpunojnë të dhënat e ofruara nga palët e treta; ose

ii. t'u sigurojnë direkt operatorëve të avionëve të dhënat që do të përdoren për qëllime operacionale.

Parashikimet në këtë shkronjë zbatohen nga data 27 mars 2031, me kusht që rregullorja që përcakton kërkesat për ofrimin e sigurt të shërbimeve të përpunimit në tokë dhe për organizatat që i ofrojnë ato, përafrim i rregullores së deleguar të Komisionit (BE) 2025/20 të ketë hyrë në fuqi.

2. Kjo Rregullore nuk cenon kërkesat e sigurisë së informacionit dhe sigurisë kibernetike të përcaktuara në VKM-në nr. 411, datë 19.6.2024, "Për miratimin e Programit Kombëtar të Sigurisë së Aviacionit Civil", dhe në legjislacioni në fuqi për sigurinë kibernetike.

Neni 3

Përkufizimet

Për qëllim të kësaj Rregulloreje, zbatohen përkufizimet e mëposhtme:

1. "Siguria e informacionit" nënkupton ruajtjen e konfidencialitetit, integritetit, autenticitetit dhe disponueshmërisë së rrjetit dhe sistemeve të informacionit;

2. "Ngjarja e sigurisë së informacionit" nënkupton një ndodhi të identifikuar të një sistemi, shërbimi ose gjendje rrjeti që tregon një shkelje të mundshme të politikës së sigurisë së informacionit ose dështimin e kontrolleve të sigurisë së informacionit, ose një situatë të panjohur më parë që mund të jetë e rëndësishme për sigurinë e informacionit;

3. "Incident" është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara, ose të shërbimeve të ofruara apo të aksesueshme përmes rrjeteve dhe sistemeve të informacionit;

4. "Rreziku i sigurisë së informacionit" nënkupton rrezikun për operimet organizative të aviacionit civil, asetet, individët dhe organizatat e tjera, për shkak të potencialit të një ngjarjeje të sigurisë së informacionit. Rreziqet e sigurisë së informacionit shoqërohen me mundësinë që kërcënimet të shfrytëzojnë dobësitë e një aseti informacioni ose një grupi asetesh informacioni;

5. “Kërcënim” nënkupton një shkelje të mundshme të sigurisë së informacionit që ekziston kur ekziston një entitet, rrethanë, veprim ose ngjarje që mund të shkaktojë dëm.

6. “Vulnerabilitet” nënkupton një defekt ose cenueshmëri në një aset ose një sistem, procedura, projektim, zbatim ose masa të sigurisë së informacionit që mund të shfrytëzohen dhe që rezulton në një thyerje ose shkelje të politikës së sigurisë së informacionit.

Neni 4

Kërkesat që dalin nga legjislacioni tjetër kombëtar

1. Kur një organizatë e përmendur në nenin 2 përputhet me kërkesat e sigurisë specifike kombëtare në lidhje me masat për një nivel të lartë të sigurisë kibernetike që janë ekuivalente me kërkesat e përcaktuara në këtë Rregullore, pajtueshmëria me këto kërkesa sigurie do të konsiderohet se përbën përputhje me kërkesat e përcaktuara në këtë Rregullore.

2. Kur një organizatë e përmendur në nenin 2 është një operator ose një ent i referuar në programet kombëtare të sigurisë së aviacionit civil të përcaktuara në përputhje me nenin 10 të udhëzimit nr. 26, datë 20.10.2010, “Mbi rregullat e përgjithshme në fushën e sigurisë së Aviacionit Civil”, kërkesat e sigurisë kibernetike të përfshira në VKM-në nr. 411, datë 19.6.2024, “Për miratimin e Programit Kombëtar të Sigurisë së Aviacionit Civil”, konsiderohen të jenë ekuivalente me kërkesat e përcaktuara në këtë Rregullore, me përjashtim të pikës IS.D.OR.230 të aneksit të kësaj Rregulloreje, e cila duhet të respektohet.

3. Ministri pas konsultimit me Autoritetin e Aviacionit Civil dhe me Autoritetin përgjegjës për Sigurinë Kibernetike, mund të miratojë udhëzime për vlerësimin e ekuivalencës së kërkesave të përcaktuara në këtë Rregullore dhe rregullat kombëtare në lidhje me masat për një nivel të lartë të sigurisë kibernetike.

Neni 5

Autoriteti kompetent

1. Autoriteti përgjegjës për certifikimin dhe mbikëqyrjen e pajtueshmërisë me këtë Rregullore do të jetë:

a) në lidhje me organizatat e përmendura në nenin 2, shkronja “a”, autoriteti kompetent i caktuar në përputhje me aneksin I (pjesa 21) të urdhrit të ministrit nr. 57, datë 13.3.2024, “Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor, ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesat e aftësisë së organizatave të projektimit dhe prodhimit”.

b) në lidhje me organizatat e përmendura në nenin 2, shkronja “b”, autoriteti kompetent i caktuar në përputhje me aneksin III (pjesa-ADR.OR) të urdhrit të ministrit nr. 170, datë 13.9.2022, “Për miratimin e rregullores për përcaktimin e kërkesave dhe procedurave administrative që lidhen me aerodromet në Republikën e Shqipërisë”, i ndryshuar.

c) në lidhje me organizatat e përmendura në nenin 2, shkronja “c”, autoriteti kompetent i caktuar në përputhje me aneksin (pjesa-ARGH) të Rregullores, që përcakton rregullat për zbatimin e VKM-së nr. 1095/2020, i ndryshuar, në lidhje me kërkesat për mbikëqyrjen e shërbimeve të

përpunimit në tokë dhe organizatave që i ofrojnë ato, që përafron e rregullores zbatuese të Komisionit (BE) 2025/23.

Parashikimet në këtë shkronjë zbatohen nga data 27 mars 2031, me kusht që rregullorja që përcakton rregullat për zbatimin e VKM-së nr. 1095/2020, e ndryshuar, në lidhje me kërkesat për mbikëqyrjen e shërbimeve të përpunimit në tokë dhe organizatave që i ofrojnë ato, përafrim i rregullores zbatuese të Komisionit (BE) 2025/23, të ketë hyrë në fuqi.

2. Në rast se legjislacioni kombëtar, për qëllimet e kësaj Rregulloreje, përcakton një entitet të pavarur dhe autonom për të përmbushur rolin dhe përgjegjësitë e caktuara të autoriteteve kompetente të përmendura në pikën 1, masat e koordinimit do të vendosen ndërmjet atij entiteti dhe autoriteteve kompetente, e përmendura në pikën 1, për të siguruar mbikëqyrje efektive të të gjitha kërkesave që duhet të përmbushen nga organizatat.

ANEKSI
SIGURIA E INFORMACIONIT – KËRKESAT E ORGANIZATËS
[PJESA-IS.D.OR]

IS.D.OR.100 Fushëveprimi
IS.D.OR.200 Sistemi i menaxhimit të sigurisë së informacionit
IS.D.OR.205 Vlerësimi i rrezikut të sigurisë së informacionit
IS.D.OR.210 Trajtimi i rrezikut të sigurisë së informacionit
IS.D.OR.215 Skema e raportimit të brendshëm të sigurisë së informacionit
IS.D.OR.220 Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi
IS.D.OR.225 Përgjigjja ndaj gjetjeve të njoftuara nga autoriteti kompetent
IS.D.OR.230 Skema e raportimit të jashtëm të sigurisë së informacionit
IS.D.OR.235 Kontraktimi i aktiviteteve të menaxhimit të sigurisë së informacionit
IS.D.OR.240 Kërkesat për personelin
IS.D.OR.245 Ruajtja e të dhënave
IS.D.OR.250 Manuali i menaxhimit të sigurisë së informacionit (ISMM)
IS.D.OR.255 Ndryshimet në sistemin e menaxhimit të sigurisë së informacionit
IS.D.OR.260 Përmirësim i vazhdueshëm

IS.D.OR.100 Fushëveprimi

Kjo pjesë përcakton kërkesat që duhet të plotësojnë organizatat e përmendura në nenin 2 të kësaj Rregulloreje.

IS.D.OR.200 Sistemi i menaxhimit të sigurisë së informacionit (ISMS)

a) Për të arritur objektivat e përcaktuar në nenin 1, organizata duhet të krijojë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit (ISMS), i cili siguron që organizata:

1. vendos një politikë për sigurinë e informacionit duke përcaktuar parimet e përgjithshme të organizatës në lidhje me ndikimin e mundshëm të rreziqeve të sigurisë së informacionit në sigurinë në operim;

2. identifikon dhe rishikon rreziqet e sigurisë së informacionit në përputhje me pikën IS.D.OR.205;

3. përcakton dhe zbaton masat e trajtimit të rrezikut të sigurisë së informacionit, në përputhje me pikën IS.D.OR.210;

4. zbaton një skemë raportimi të brendshëm të sigurisë së informacionit, në përputhje me pikën IS.D.OR.215;

5. përcakton dhe zbaton, në përputhje me pikën IS.D.OR.220, masat e nevojshme për zbulimin e ngjarjeve të sigurisë së informacionit, identifikon ato ngjarje që konsiderohen si incidente me një ndikim të mundshëm në sigurinë në operim dhe u përgjigjet dhe rikuperohet nga këto incidente të sigurisë së informacionit;

6. zbaton masat që janë njoftuar nga autoriteti kompetent si reagim i menjëhershëm ndaj një incidenti ose cenueshmërie të sigurisë së informacionit me ndikim në sigurinë në operim;

7. merr masat e duhura, në përputhje me pikën IS.D.OR.225, për të adresuar gjetjet e njoftuara nga autoriteti kompetent;

8. zbaton një skemë raportimi të jashtëm në përputhje me pikën IS.D.OR.230 për t'i dhënë mundësi autoritetit kompetent të ndërmarrë veprimet e duhura;

9. përputhet me kërkesat e përfshira në pikën IS.D.OR.235, kur kontrakton ndonjë pjesë të aktiviteteve të përmendura në pikën IS.D.OR.200 me organizata të tjera;

10. përputhet me kërkesat e personelit të përcaktuara në pikën IS.D.OR.240;

11. përputhet me kërkesat e mbajtjes së të dhënave të përcaktuara në pikën IS.D.OR.245;

12. monitoron përputhshmërinë e organizatës me kërkesat e kësaj rregulloreje dhe jep komente mbi gjetjet te menaxheri përgjegjës ose, në rastin e organizatave projektuese, te drejtuesi i organizatës projektuese, me qëllim që të sigurojë zbatimin efektiv të veprimeve korrigjuese;

13. mbron, pa paragjykuar kërkesat e zbatueshme të raportimit të incidentit, konfidencialitetin e çdo informacioni që organizata mund të ketë marrë nga organizata të tjera, sipas nivelit të saj të ndjeshmërisë.

b) Për të përmbushur vazhdimisht kërkesat e referuara në nenin 1, organizata zbaton një proces përmirësimi të vazhdueshëm në përputhje me pikën IS.D.OR.260.

c) Organizata dokumenton, në përputhje me pikën IS.D.OR.250, të gjitha proceset kryesore, procedurat, rolet dhe përgjegjësitë e kërkuara për të qenë në përputhje me pikën IS.D.OR.200(a) dhe krijon një proces për ndryshimin e këtij dokumentacioni. Ndryshimet në këto procese, procedura, role dhe përgjegjësi menaxhohen në përputhje me pikën IS.D.OR.255.

d) Proceset, procedurat, rolet dhe përgjegjësitë e vendosura nga organizata në përputhje me pikën IS.D.OR.200(a) do të korrespondojnë me natyrën dhe kompleksitetin e aktiviteteve të saj, bazuar në një vlerësim të rreziqeve të sigurisë së informacionit të qenësishme për këto aktivitete dhe mund të integrohen brenda sistemeve të tjera ekzistuese të menaxhimit të zbatuara tashmë nga organizata.

e) Pa paragjykuar detyrimin për të përmbushur kërkesat e raportimit të përfshira në urdhrin e ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë" dhe kërkesat e pikës IS.D.OR.200 (a)(13), organizatës mund t'i jepet miratimi nga autoriteti kompetent për të mos zbatuar kërkesat e përmendura në shkronjat "a" deri në "d" dhe kërkesat përkatëse të përfshira në pikat IS.D.OR.205 përmes IS.D.OR.260, nëse tregon në bindjen e këtij autoriteti se aktivitetet, objektet dhe burimet e saj, si dhe shërbimet që ajo operon, ofron, merr dhe mirëmban, nuk paraqesin ndonjë rrezik sigurie informacioni me një ndikim të mundshëm mbi sigurinë në operim as për veten e as për organizatat e tjera. Miratimi bazohet në një vlerësim të dokumentuar të rrezikut të sigurisë së informacionit të kryer nga organizata ose një palë e tretë në përputhje me pikën IS.D.OR.205 dhe të rishikuar dhe miratuar nga autoriteti i saj kompetent.

Vlefshmëria e vazhdueshme e atij miratimi rishikohet nga autoriteti kompetent pas ciklit të zbatueshëm të auditimit të mbikëqyrjes dhe sa herë që zbatohen ndryshime në fushën e punës së organizatës.

IS.D.OR.205 Vlerësimi i rrezikut të sigurisë së informacionit

a) Organizata duhet të identifikojë të gjitha elementet e saj, të cilat mund të ekspozohen ndaj rreziqeve të sigurisë së informacionit. Kjo përfshin:

1. aktivitetet, objektet dhe burimet e organizatës, si dhe shërbimet që organizata operon, ofron, merr ose mirëmban;

2. pajisjet, sistemet, të dhënat dhe informacionet që kontribuojnë në funksionimin e elementeve të renditura në pikën 1.

b) Organizata duhet të identifikojë ndërlidhjet që ajo ka me organizatat e tjera dhe të cilat mund të rezultojnë në ekspozimin e ndërsjellë ndaj rreziqeve të sigurisë së informacionit.

c) Në lidhje me elementet dhe ndërlidhjet e përmendura në shkronjat "a" dhe "b", organizata duhet të identifikojë rreziqet e sigurisë së informacionit, që mund të kenë një ndikim të mundshëm në sigurinë në operim. Për çdo rrezik të identifikuar, organizata duhet:

1. të caktojë një nivel rreziku sipas një klasifikimi të paracaktuar të vendosur nga organizata;

2. të lidhë çdo rrezik dhe nivelin e tij me elementin ose ndërlidhjen përkatëse të identifikuar në përputhje me shkronjat "a" dhe "b".

Klasifikimi i paracaktuar i referuar në pikën 1 do të marrë parasysh potencialin e shfaqjes së skenarit të kërcënimit dhe ashpërsinë e pasojave të tij të sigurisë. Bazuar në atë klasifikim, dhe duke marrë parasysh nëse organizata ka një proces të strukturuar dhe të përsëritshëm të menaxhimit të rrezikut për operimet, organizata duhet të jetë në gjendje të përcaktojë nëse rreziku është i pranueshëm ose duhet të trajtohet në përputhje me pikën IS.D.OR.210.

Për të lehtësuar krahasueshmërinë e ndërsjellë të vlerësimeve të rreziqeve, caktimi i nivelit të rrezikut në përputhje me pikën 1 do të marrë parasysh informacionin përkatës të marrë në koordinim me organizatat e përmendura në shkronjën "b".

d) Organizata duhet të rishikojë dhe përditësojë vlerësimin e rrezikut të kryer në përputhje me shkronjat "a", "b" dhe "c" në cilëndo nga situatat e mëposhtme:

1. ka një ndryshim në elementet që u nënshtrohen rreziqeve të sigurisë së informacionit;

2. ka një ndryshim në lidhjet ndërmjet organizatës dhe organizatave të tjera, ose në rreziqet e komunikuara nga organizatat e tjera;

3. ka një ndryshim në informacionin ose njohuritë e përdorura për identifikimin, analizën dhe klasifikimin e rreziqeve;

4. ka mësime të nxjerra nga analiza e incidenteve të sigurisë së informacionit.

IS.D.OR.210 Trajtimi i rrezikut të sigurisë së informacionit

a) Organizata duhet të zhvillojë masa për të trajtuar rreziqet e papranueshme të identifikuara në përputhje me pikën IS.D.OR.205, t'i zbatojë ato në kohën e duhur dhe të kontrollojë efektivitetin e tyre të vazhdueshëm. Këto masa do t'i mundësojnë organizatës, që të:

1. Kontrollojë rrethanat që kontribuojnë në shfaqjen efektive të skenarit të kërcënimit;

2. Zvogëlojë pasojat në sigurinë e aviacionit që lidhen me materializimin e skenarit të kërcënimit;

3. Shmangë rreziqet.

Këto masa nuk do të sjellin ndonjë rrezik të ri të mundshëm të papranueshëm për sigurinë në operim.

b) Personi i përmendur në pikën IS.D.OR.240(a) dhe (b) dhe personeli tjetër i prekur i organizatës duhet të informohet për rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.D.OR.205, skenarët përkatës të kërcënimit dhe masat që duhen zbatuar.

Organizata duhet, gjithashtu, të informojë organizatat me të cilat ka një ndërlidhje në përputhje me pikën IS.D.OR.205(b) për çdo rrezik të ndarë midis të dyja organizatave.

IS.D.OR.215 Skema e raportimit të brendshëm të sigurisë së informacionit

a) Organizata krijon një skemë të brendshme raportimi për të mundësuar mbledhjen dhe vlerësimin e ngjarjeve të sigurisë së informacionit, duke përfshirë ato që do të raportohen në përputhje me pikën IS.D.OR.230.

b) Kjo skemë dhe procesi i përmendur në pikën IS.D.OR.220 i mundëson organizatës, që të:

1. identifikojë se cilat nga ngjarjet e raportuara në përputhje me shkronjën "a" konsiderohen si incidente ose cenueshmëri të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim;

2. identifikojë shkaqet dhe faktorët që kontribuojnë në incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën 1, dhe adresojë ato si pjesë e procesit të menaxhimit të rrezikut të sigurisë së informacionit në përputhje me pikat IS.D.OR.205 dhe IS.D.OR.220;

3. sigurojë një vlerësim të të gjithë informacionit të njohur, përkatës në lidhje me incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën 1;

4. sigurojë zbatimin e një metode për shpërndarjen e brendshme të informacionit sipas nevojës.

c) Çdo organizate të kontraktuar e cila mund ta ekspozojë organizatën ndaj rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë e aviacionit do t'i kërkohet të raportojë ngjarjet e sigurisë së informacionit tek organizata. Këto raporte do të dorëzohen duke përdorur procedurat e përcaktuara në marrëveshjet specifike kontraktuale dhe do të vlerësohen në përputhje me shkronjën "b".

d) Organizata bashkëpunon në hetime me çdo organizatë tjetër që ka një kontribut të rëndësishëm në sigurinë e informacionit të aktiviteteve të saj.

e) Organizata mund ta integrojë atë skemë raportimi me skema të tjera raportimi që ajo ka zbatuar tashmë.

IS.D.OR.220 Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi

a) Bazuar në rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.D.OR.205 dhe rezultatin e trajtimit të rrezikut të kryer në përputhje me pikën IS.D.OR.210, organizata do të zbatojë masat për zbulimin e incidenteve dhe dobësitë që tregojnë materializimin e mundshëm të rreziqeve të papranueshme dhe që mund të kenë një ndikim të mundshëm në sigurinë në operim. Këto masa zbulimi do t'i mundësojnë organizatës, që të:

1. identifikojë devijimet nga linjat bazë të performancës funksionale të paracaktuara;

2. aktivizojë paralajmërimet për të aktivizuar masat e duhura të reagimit, në rast të ndonjë devijimi.

b) Organizata do të zbatojë masa për t'iu përgjigjur çdo kushti ngjarjeje të identifikuar në përputhje me shkronjën "a" që mund të zhvillohet ose të jetë shndërruar në një incident të sigurisë së informacionit. Këto masa reagimi do t'i mundësojnë organizatës, që të:

1. iniciojë reagimin ndaj paralajmërimeve të përmendura në pikën (a)(2), duke aktivizuar burimet dhe kursin e veprimeve të paracaktuara;

2. përmbajë përhapjen e një sulmi dhe të shmangë materializimin e plotë të një skenari kërcënimi;

3. kontrollojë mënyrën e dështimit të elementeve të prekura të përcaktuara në pikën IS.D.OR.205(a).

c) Organizata zbaton masa që synojnë rikuperimin nga incidentet e sigurisë së informacionit, duke përfshirë masat emergjente, nëse është e nevojshme. Këto masa rikuperimi do t'i mundësojnë organizatës, që të:

1. heqë gjendjen që shkaktoi incidentin, ose kufizojë atë në një nivel të tolerueshëm;

2. arrijë një gjendje të sigurt të elementeve të prekura të përcaktuara në pikën IS.D.OR.205(a), brenda një kohe rikuperimi të përcaktuar më parë nga organizata.

IS.D.OR.225 Përgjigje ndaj gjetjeve të njoftuara nga autoriteti kompetent

a) Pas marrjes së njoftimit për gjetjet e dorëzuara nga autoriteti kompetent, organizata duhet të:

1. identifikojë shkakun kryesor ose shkaqet dhe faktorët që kontribuojnë në mospërputhje;

2. përcaktojë një plan veprimi korrigjues;

3. demonstrojë korrigjimin e mospërputhshmërisë sipas dëshirës së autoritetit kompetent.

b) Veprimet e përmendura në shkronjën "a" kryhen brenda periudhës së rënë dakord me autoritetin kompetent.

IS.D.OR.230 Skema e raportimit të jashtëm të sigurisë së informacionit

a) Organizata zbaton një sistem raportimi për sigurinë e informacionit që përputhet me kërkesat e përcaktuara në urdhrin e ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë", dhe çdo ndryshim i tij nëse kjo Rregullore është e zbatueshme për organizatën.

b) Pa cenuar detyrimet e urdhrit të ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë", organizata duhet të sigurojë që çdo incident ose cenueshmëri e sigurisë së informacionit, që mund të përfaqësojë një rrezik të rëndësishëm për sigurinë e aviacionit, t'i raportohet autoritetit të tyre kompetent. Për më tepër:

1. kur një incident ose cenueshmëri e tillë prek një avion ose sistem ose përbërës të lidhur, organizata duhet t'ia raportojë, gjithashtu, mbajtësit të miratimit të projektimit;

2. kur një incident ose cenueshmëri e tillë prek një sistem ose përbërës të përdorur nga organizata, organizata duhet t'ia raportojë atë organizatës përgjegjëse për hartimin e sistemit ose përbërësit.

c) Organizata duhet të raportojë kushtet e përmendura në shkronjën "b", si më poshtë:

1. një njoftim do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit ose përbërësit, sapo organizata të jetë e njohur për gjendjen;

2. një raport do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit ose përbërësit, sa më shpejt të jetë e mundur, por jo më shumë se 72 orë nga koha kur organizata është vënë në dijeni për rrethanën, përveç rasteve kur rrethanat e jashtëzakonshme e pengojnë këtë.

Raporti do të bëhet në formën e përcaktuar nga autoriteti kompetent dhe do të përmbajë të gjithë informacionin përkatës për gjendjen e njohur për organizatën;

3. një raport vijues do t'i dorëzohet autoritetit kompetent dhe, nëse është e aplikueshme, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit ose përbërësit, duke ofruar detaje të veprimeve që organizata ka ndërmarrë ose synon të ndërmarrë për t'u rimëkëmbur nga incidenti dhe veprimet që synon të ndërmarrë për të parandaluar incidente të ngjashme të sigurisë së informacionit në të ardhmen.

Raporti vijues do të dorëzohet sapo të jenë identifikuar këto veprime dhe do të përgatitet në formën e përcaktuar nga autoriteti kompetent.

IS.D.OR.235 Kontraktimi i aktiviteteve të menaxhimit të sigurisë së informacionit

a) Organizata duhet të sigurojë që kur kontrakton ndonjë pjesë të aktiviteteve të përmendura në pikën IS.D.OR.200 me organizata të tjera, aktivitetet e kontraktuara janë në përputhje me kërkesat e kësaj Rregulloreje dhe organizata e kontraktuar punon nën mbikëqyrjen e saj. Organizata duhet të sigurojë që rreziqet që lidhen me aktivitetet e kontraktuara të menaxhohen siç duhet.

b) Organizata duhet të sigurojë që autoriteti kompetent mund të ketë akses me kërkesë të organizatës së kontraktuar për të përcaktuar pajtueshmërinë e vazhdueshme me kërkesat e zbatueshme të përcaktuara në këtë Rregullore.

IS.D.OR.240 Kërkesat për personelin

a) Menaxheri përgjegjës i organizatës ose, në rastin e organizatave projektuese, drejtuesi i organizatës së projektimit, i caktuar në përputhje me urdhrin e ministrit nr. 57, datë 13.3.2024, "Për miratimin e Rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesat e aftësisë së organizatave të projektimit dhe prodhimit" dhe urdhrit të ministrit nr. 170, datë 13.9.2022, "Për miratimin e rregullores për përcaktimin e kërkesave dhe procedurave administrative që lidhen me aerodromet në Republikën e Shqipërisë", të ndryshuar, i përmendur në shkronjat "a" dhe "b" të nenit 2 të kësaj Rregulloreje, do të ketë autoritetin e korporatës për të siguruar që të gjitha aktivitetet e kërkuara nga kjo Rregullore mund të financohen dhe kryhen.

Ai person do të:

1. sigurojë që të gjitha burimet e nevojshme janë në dispozicion për të përmbushur kërkesat e kësaj Rregulloreje;

2. krijojë dhe promovojë politikën e sigurisë së informacionit të përmendur në pikën IS.D.OR.200(a)(1);

3. demonstrojë një kuptim të mirë të kësaj Rregulloreje.

b) Menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës së projektimit, cakton një person ose grup personash për të siguruar që organizata është në përputhje me kërkesat e kësaj rregulloreje dhe përcakton shtrirjen e autoritetit të tyre. Ai person ose grup personash duhet t'i raportojë drejtpërdrejt menaxherit përgjegjës ose, në rastin e organizatave të projektimit, kreut të organizatës projektuese dhe duhet të ketë njohuritë, përgatitjen dhe përvojën e duhur për të përmbushur përgjegjësitë përkatëse. Në procedurë do të përcaktohet se kush e zëvendëson një person të caktuar në rast të mungesës së gjatë të atij personi.

c) Menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës së projektimit do të emërojë një person ose grup personash me përgjegjësi për të menaxhuar funksionin e monitorimit të pajtueshmërisë të përmendur në pikën IS.D.OR.200(a)(12).

d) Kur organizata ndan strukturat organizative, politikat, proceset dhe procedurat e sigurisë së informacionit, me organizata të tjera ose me zona të organizatës së tyre që nuk janë pjesë e miratimit ose deklaratës, menaxheri përgjegjës ose, në rastin e organizatave projektuese, drejtuesi i organizatës projektuese, mund t'ia delegojë aktivitetet e saj një personi të përbashkët përgjegjës.

Në një rast të tillë, masat e koordinimit do të vendosen ndërmjet menaxherit përgjegjës të organizatës ose, në rastin e organizatave projektuese, kreut të organizatës projektuese dhe personit të përbashkët përgjegjës për të siguruar integrimin e duhur të menaxhimit të sigurisë së informacionit brenda organizatës.

e) Menaxheri përgjegjës ose drejtuesi i organizatës së projektimit, ose personi përgjegjës i përbashkët i përmendur në shkronjën "d", ka autoritetin e korporatës për të krijuar dhe mirëmbajtur strukturat organizative, politikat, proceset dhe procedurat e nevojshme për zbatimin e pikës IS.D.OR.200.

f) Organizata duhet të ketë një proces të vendosur për të siguruar që ka personel të mjaftueshëm në detyrë për të kryer aktivitetet e mbuluara nga ky aneks.

g) Organizata duhet të ketë një proces të vendosur për të siguruar që personeli i përmendur në shkronjën "f" të ketë kompetencën e nevojshme për të kryer detyrat e tyre.

h) Organizata duhet të ketë një proces të vendosur për të siguruar që personeli të pranojë përgjegjësitë që lidhen me rolet dhe detyrat e caktuara.

i) Organizata duhet të sigurojë që identiteti dhe besueshmëria e personelit që ka akses në sistemet e informacionit dhe të dhënat që u nënshtrohen kërkesave të kësaj Rregulloreje janë përcaktuar siç duhet.

IS.D.OR.245 Ruajtja e të dhënave

a) Organizata duhet të regjistrojë të dhënat për aktivitetet e saj të menaxhimit të sigurisë së informacionit

1. Organizata duhet të sigurojë që të dhënat e mëposhtme janë të arkivuara dhe të gjurmueshme:

i. çdo miratim i marrë dhe çdo vlerësim shoqërues i rrezikut të sigurisë së informacionit në përputhje me pikën IS.D.OR.200(e);

ii. kontratat për aktivitetet e përmendura në pikën IS.D.OR.200(a)(9);

iii. regjistrimet e proceseve kryesore të përmendura në pikën IS.D.OR.200(d);

iv. të dhënat e rreziqeve të identifikuara në vlerësimin e rrezikut të përmendur në pikën IS.D.OR.205 së bashku me masat shoqëruese të trajtimit të rrezikut të përmendura në pikën IS.D.OR.210;

v. të dhënat e incidenteve dhe cenueshmërive të sigurisë së informacionit të raportuara në përputhje me skemat e raportimit të përmendura në pikat IS.D.OR.215 dhe IS.D.OR.230;

vi. të dhënat e atyre ngjarjeve të sigurisë së informacionit që mund të kenë nevojë të rivlerësohen për të zbuluar incidente ose cenueshmëri të pazbuluara të sigurisë së informacionit.

2. Regjistrimet e përmendura në pikën (1)(i) mbahen të paktën deri në 5 vjet pasi miratimi të ketë humbur vlefshmërinë e tij.

3. Të dhënat e përmendura në pikën (1)(ii) mbahen të paktën deri në 5 vjet pas ndryshimit ose përfundimit të kontratës.

4. Të dhënat e përmendura në pikën (1)(iii), (iv) dhe (v) mbahen të paktën për një periudhë prej 5 vjetësh.

5. Regjistrimet e përmendura në pikën (1)(vi) mbahen derisa ato ngjarje të sigurisë së informacionit të rivlerësohen në përputhje me një periodicitet të përcaktuar në një procedurë të vendosur nga organizata.

b) Organizata duhet të mbajë shënime për kualifikimin dhe përvojën e stafit të vet të përfshirë në aktivitetet e menaxhimit të sigurisë së informacionit

1. të dhënat e kualifikimit dhe përvojës së personelit ruhen për aq kohë sa personi punon për organizatën dhe për të paktën 3 vjet pasi personi të jetë larguar nga organizata;

2. anëtarëve të personelit, me kërkesën e tyre, u jepet akses në të dhënat e tyre individuale; përveç kësaj, me kërkesën e tyre, organizata do t'u sigurojë atyre një kopje të të dhënave të tyre individuale pas largimit nga organizata.

c) Formati i të dhënave specifikohet në procedurat e organizatës.

d) Regjistrimet ruhen në një mënyrë që siguron mbrojtje nga dëmtimi, ndryshimi dhe vjedhja, me informacionin që identifikohet, kur kërkohet, sipas nivelit të klasifikimit të sigurisë. Organizata duhet të sigurojë që të dhënat të ruhen duke përdorur mjete për të siguruar integritetin, autenticitetin dhe aksesin e autorizuar.

IS.D.OR.250 Manuali i menaxhimit të sigurisë së informacionit (ISMM)

a) Organizata duhet t'i vërë në dispozicion autoritetit kompetent një manual për menaxhimin e sigurisë së informacionit (ISMM) dhe, kur është e aplikueshme, çdo manual dhe procedurë të lidhur me referencë, që përmban:

1. një deklaratë të nënshkruar nga menaxheri përgjegjës ose, në rastin e organizatave projektuese, nga drejtuesi i organizatës së projektimit, që konfirmon se organizata do të punojë në çdo kohë në përputhje me këtë aneks dhe me ISMM-në; nëse menaxheri përgjegjës ose, në rastin e organizatave të projektimit, drejtuesi i organizatës së projektimit, nuk është shefi ekzekutiv (CEO) i organizatës, atëherë CEO i tillë duhet të kundërfirmojë deklaratën;

2. titujt, emrat, detyrat, përgjegjësitë, përgjegjësitë dhe autoritetet e personit ose personave të përmendur në pikën IS.D.OR.240(b) dhe (c);

3. titullin, emrin, detyrat, përgjegjësitë dhe autoritetet e personit përgjegjës të përbashkët të përmendur në pikën IS.D.OR.240(d), nëse është e aplikueshme;

4. politikën e sigurisë së informacionit të organizatës, siç referohet në pikën IS.D.OR.200(a)(1);

5. një përshkrim të përgjithshëm të numrit dhe kategorive të personelit dhe të sistemit të vendosur për të planifikuar disponueshmërinë e personelit, siç kërkohet nga pika IS.D.OR.240;

6. titujt, emrat, detyrat, përgjegjësitë dhe autoritetet e personave kyç përgjegjës për zbatimin e pikës IS.D.OR.200, duke përfshirë personin ose personat përgjegjës për funksionin e monitorimit të pajtueshmërisë të përmendur në pika IS.D.OR.200(a)(12);

7. një organigramë që tregon zinxhirët shoqërues të llogaridhënies dhe përgjegjësisë për personat e përmendur në pikat 2 dhe 6;

8. përshkrimin e skemës së raportimit të brendshëm të përmendur në pikën IS.D.OR.215;

9. procedurat që përcaktojnë se si organizata siguron përputhjen me këtë pjesë, dhe në veçanti:

i. pika e dokumentacionit IS.D.OR.200(c);

ii. procedurat që përcaktojnë se si organizata kontrollon çdo aktivitet të kontraktuar të përmendur në pikën IS.D.OR.200(a)(9);

iii. procedurën e ndryshimit të ISMM të përcaktuar në shkronjën "c";

10. detajet e mjeteve alternative të pajtueshmërisë të miratuara aktualisht.

b) Lëshimi fillestar i ISMM-së miratohet dhe një kopje mbahet nga autoriteti kompetent. Nuk kërkohet miratim për deklarimin e organizatave. ISMM ndryshohet sipas nevojës, me qëllim që të mbetet një përshkrim i përditësuar i ISMM-së së organizatës. Një kopje e çdo ndryshimi në ISMM duhet t'i jepet autoritetit kompetent.

c) Ndryshimet në ISMM menaxhohen sipas procedurës së përcaktuar nga organizata. Çdo ndryshim që nuk përfshihet në objektin e kësaj procedure dhe çdo ndryshim në lidhje me ndryshimet e përmendura në pikën IS.D.OR.255(b), miratohet nga autoriteti kompetent. Nuk kërkohet miratim për deklarimin e organizatave.

d) Organizata mund të integrojë ISMM-në me dokumente ose manuale të tjera menaxheriale që mban, me kusht që të ketë një referencë të qartë të kryqëzuar që tregon se cilat pjesë të dokumentit ose manualit të menaxhimit korrespondojnë me kërkesat e ndryshme të përfshira në këtë aneks.

IS.D.OR.255 Ndryshime në sistemin e menaxhimit të sigurisë së informacionit

a) Ndryshimet në ISMS mund të menaxhohen dhe t'i njoftohen autoritetit kompetent në një procedurë të zhvilluar nga organizata. Kjo procedurë miratohet nga autoriteti kompetent, me përjashtim të organizatave deklaruese.

b) Në lidhje me ndryshimet në ISMS që nuk mbulohen nga procedura e përmendur në shkronjën "a", organizata duhet të aplikojë dhe të marrë një miratim të lëshuar nga autoriteti kompetent, me përjashtim të organizatave deklaruese, për të cilat nuk kërkohet miratim.

Në lidhje me këto ndryshime:

1. aplikimi duhet të dorëzohet përpara se të ndodhë një ndryshim i tillë, në mënyrë që t'i mundësojë autoritetit kompetent të përcaktojë pajtueshmërinë e vazhdueshme me këtë Rregullore dhe të ndryshojë, nëse është e nevojshme, certifikatën e organizatës dhe kushtet përkatëse të miratimit që i bashkëlidhen;

2. organizata vë në dispozicion të autoritetit kompetent çdo informacion që kërkon për të vlerësuar ndryshimin;

3. ndryshimi zbatohet vetëm pas marrjes së një miratimi zyrtar nga autoriteti kompetent, me përjashtim të organizatave deklaruese, të cilat mund ta zbatojnë menjëherë ndryshimin;

4. organizata operon sipas kushteve të përcaktuara nga autoriteti kompetent gjatë zbatimit të këtyre ndryshimeve.

IS.D.OR.260 Përmirësimi i vazhdueshëm

a) Organizata vlerëson, duke përdorur tregues të përshtatshëm të performancës, efektivitetin dhe pjekurinë e ISMS-së. Ky vlerësim kryhet mbi një bazë kalendarike të paracaktuar nga organizata ose pas një incidenti të sigurisë së informacionit.

b) Nëse konstatohen mangësi pas vlerësimit të kryer në përputhje me shkronjën "a", organizata merr masat e nevojshme të përmirësimit për të siguruar që ISMS-ja të vazhdojë të jetë në përputhje me kërkesat e zbatueshme dhe të mbajë rreziqet e sigurisë së informacionit në një nivel të pranueshëm. Përveç kësaj, organizata rivlerëson ato elemente të ISMS-së, që preken nga masat e miratuara.

SHTOJCA II

RREGULLORE PËR PËRCAKTIMIN E RREGULLAVE PËR ZBATIMIN E VENDIMIT TË KËSHILLIT TË MINISTRAVE NR. 1095, DATË 24.12.2020, "PËR MIRATIMIN E KËRKESAVE THELBËSORE NË FUSHËN E AVIACIONIT CIVIL", të NDRYSHUAR, NË LIDHJE ME KËRKESAT PËR MENAXHIMIN E RREZIQEVE TË SIGURISË SË INFORMACIONIT ME NJË NDIKIM TË MUNDSHËM NË SIGURINË NË OPERIM PËR ORGANIZATAT E MBULUARA NGA URDHRAT E MINISTRIT: NR. 79, DATË 15.4.2024, NR. 80, DATË 30.6.2023, I NDRYSHUAR, NR. 178, DATË 20.12.2023, I NDRYSHUAR, NR. 171, DATË 11.11.2025, NR. 193, DATË 6.10.2022, I NDRYSHUAR, NR. 119, DATË 29.9.2023, DHE PËR AUTORITETET KOMPETENTE TË MBULUARA NGA URDHRAT E MINISTRIT: NR. 57, DATË 13.3.2024, NR. 79, DATË 15.4.2024, NR. 80, DATË 30.6.2023, I NDRYSHUAR, NR. 178, DATË 20.12.2023, I NDRYSHUAR, NR. 171, DATË 11.11.2025, NR. 170, DATË 13.9.2022, I NDRYSHUAR, NR. 193, DATË 6.10.2022, I NDRYSHUAR, NR. 119, DATË 29.9.2023

Neni 1
Objekti

Kjo Rregullore përcakton kërkesat që duhet të plotësojnë organizatat dhe autoritetet kompetente në mënyrë që:

a) të identifikojnë dhe menaxhojnë rreziqet e sigurisë së informacionit me ndikim të mundshëm në sigurinë në operim, të cilat mund të ndikojnë në sistemet e teknologjisë së informacionit dhe komunikimit dhe të dhënat e përdorura për qëllime të aviacionit civil;

b) të zbulojnë ngjarjet e sigurisë së informacionit dhe të identifikojnë ato që konsiderohen si incidente të sigurisë së informacionit me ndikim të mundshëm në sigurinë në operim,

c) t'i përgjigjen dhe të rikuperojnë këto incidente të sigurisë së informacionit.

Neni 2
Fushëveprimi

1. Kjo Rregullore zbatohet për organizatat e mëposhtme:

a) organizatat e mirëmbajtjes që i nënshtrohen seksionit A të aneksit II (pjesa-145) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra", përveç atyre të përfshira vetëm në mirëmbajtjen e avionëve në përputhje me aneksin Vb (pjesa-ML) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra";

b) organizatat e menaxhimit të vazhdueshmërisë së vlefshmërisë ajrore (CAMO) që i nënshtrohen seksionit A të aneksit Vc (pjesa-CAMO) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra", përveç atyre të përfshira vetëm në menaxhimin e vazhdueshmërisë së vlefshmërisë ajrore të avionëve në përputhje me aneksin Vb (pjesa-ML) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe

produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra";

c) operatorët ajrorë që i nënshtrohen aneksit III (pjesa-ORO) të urdhrit të ministrit nr. 80, datë 30.6.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative për operimet ajrore", të ndryshuar, me përjashtim të atyre që janë të përfshirë vetëm në përdorimin e ndonjërës nga sa vijon:

i. një avion ELA 2 siç përcaktohet në nenin 1(2), shkronja "j" të urdhrit të ministrit nr. 57, datë 13.3.2024, "Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesa të aftësisë së organizatave të projektimit dhe prodhimit";

ii. aeroplanë me një helikë me një motor me një Konfigurim Maksimal Operimi të ulëseve të pasagjerëve prej 5 ose më pak, të cilët nuk klasifikohen si avionë me motor kompleks, kur ngrihen dhe ulen në të njëjtin aerodrom, ose vend operimi dhe operojnë sipas Rregullave të Fluturimit Vizual (VFR) sipas rregullave të ditës;

iii. helikopterë me një motor me një konfigurim maksimal operimi të ulëseve të pasagjerëve prej 5 ose më pak që nuk klasifikohen si avionë kompleksë me motor, kur ngrihen dhe ulen në të njëjtin aerodrom ose vend operimi dhe operojnë nën VFR sipas rregullave të ditës.

d) Organizatat e miratuara të trajnimit (ATO) që i nënshtrohen aneksit VII (pjesa-ORA) të urdhrit të ministrit nr. 178, datë 20.12.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative në lidhje me ekuipazhin ajror të aviacionit civil", të ndryshuar, përveç atyre të përfshira vetëm në aktivitetet e trajnimit të avionëve ELA2, siç përcaktohet në nenin 1, pika 2, shkronja "j" të urdhrit të ministrit nr. 57, datë 13.3.2024, "Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesa të aftësisë së organizatave të projektimit dhe prodhimit", ose të përfshira vetëm në trajnimin teorik;

e) qendrat aeromjekësore të ekuipazheve ajrore që i nënshtrohen aneksit VII (pjesa-ORA) të urdhrit të ministrit nr. 178, datë 20.12.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative në lidhje me ekuipazhin ajror të aviacionit civil", të ndryshuar;

f) operatorët e pajisjeve të trajnimit të simulimit të fluturimit (FSTD) që i nënshtrohen aneksit VII (pjesa-ORA) të urdhrit të ministrit nr. 178, datë 20.12.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative në lidhje me ekuipazhin ajror të aviacionit civil", të ndryshuar, përveç atyre të përfshira vetëm në operimin e FSTD-ve për avionët ELA2, siç përcaktohet në nenin 1 (2), shkronja "j", të urdhrit të ministrit nr. 57, datë 13.3.2024, "Për miratimin e rregullores për përcaktimin e rregullave zbatuese të vlefshmërisë ajrore dhe të certifikimit mjedisor ose deklaratën e përputhshmërisë së avionit dhe produkteve të lidhura me to, pjesëve dhe pajisjeve, si dhe për kërkesa të aftësisë së organizatave të projektimit dhe prodhimit";

g) organizatat e trajnimit të kontrollorëve të trafikut ajror (ATCO TO) dhe qendrat aeromjekësore ATCO që i nënshtrohen aneksit III (pjesa KTA.OR) të urdhrit të ministrit nr. 171, datë 11.11.2025, "Për miratimin e rregullores mbi përcaktimin e kërkesave teknike edhe procedurave administrative në lidhje me licencat dhe certifikatat e kontrollorëve të trafikut ajror";

h) organizatat që i nënshtrohen aneksit III (pjesa-ATM/ANS.OR) të urdhrit të ministrit nr. 193, datë 6.10.2022, "Për miratimin e rregullores për përcaktimin e kërkesave të përbashkëta për ofruesit e shërbimeve të menaxhimit të trafikut ajror dhe të lundrimit ajror, si dhe funksionet e

tjera të rrjetit të menaxhimit të trafikut ajror dhe mbikëqyrjen e tyre", të ndryshuar, me përjashtim të ofruesve të shërbimeve në vijim:

i. ofruesit e shërbimeve të lundrimit ajror që mbajnë një certifikatë të kufizuar në përputhje me pikën ATM/ANS.OR.A.010 të atij aneksi;

ii. ofruesit e shërbimit të informacionit të fluturimit që deklarojnë aktivitetet e tyre në përputhje me pikën ATM/ANS.OR.A.015 të atij aneksi;

i) ofruesit e shërbimeve të hapësirës – U dhe ofruesit e vetëm të përbashkët të shërbimeve të informacionit që i nënshtrohen urdhrit të ministrit nr. 119, datë 29.9.2023, "Për miratimin e rregullores mbi kuadrin rregullator për hapësirën – U të hapësirës ajrore".

j) organizatat e miratuara të përfshira në projektimin ose prodhimin e sistemeve ATM/ANS dhe përbërësve ATM/ANS që i nënshtrohen shtojcës II mbi rregulloren që përcakton kërkesat teknike dhe procedurat administrative për miratimin e organizatave të përfshira në projektimin, ose prodhimin e sistemeve dhe përbërësve të menaxhimit të trafikut ajror/shërbimeve të lundrimit ajror, që përafron rregulloren zbatuese të Komisionit (BE) 2023/1769, të urdhrit të ministrit nr. 40, datë 12.3.2025.

2. Kjo rregullore zbatohet për Autoritetin e Aviacionit Civil, kur ai është përcaktuar si autoritet kompetente, referuar nenit 6 të kësaj Rregulloreje dhe nenit 5 të Rregullores për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, "Për miratimin e kërkesave thelbësore në fushën e aviacionit civil", të ndryshuar, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhrit të ministrit nr. 57, datë 13.3.2024 dhe urdhrit të ministrit nr. 170, datë 13.9.2022, i ndryshuar, që përafron Rregulloren e Deleguar të Komisionit (BE) 2022/1645, sipas shtojcës I të këtij urdhri apo urdhrave të ministrit ku referon ky nen.

3. Kjo Rregullore zbatohet, gjithashtu, për Autoritetin e Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent përgjegjës për lëshimin, vazhdimin, ndryshimin, pezullimin ose heqjen e licencave të mirëmbajtjes së avionëve në përputhje me aneksin III (pjesa-66) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra".

3a. Kjo Rregullore zbatohet, gjithashtu, për Autoritetin e Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent përgjegjës për mbikëqyrjen e vazhdueshmërisë së vlefshmërisë ajrore të sistemeve të avionëve pa pilot individuale (UA) dhe për lëshimin e certifikatave të tyre të rishikimit të vlefshmërisë ajrore sipas Rregullores për përcaktimin e kërkesave për autoritetin kompetent dhe procedurave administrative për certifikimin, mbikëqyrjen dhe zbatimin e vlefshmërisë së vazhdueshme të sistemeve të avionëve pa pilot të certifikuar, që përafron Rregulloren Evropiane 2024/1109, si dhe për mbikëqyrjen e një organizate, siç përcaktohet në Rregulloren që përcakton rregullat e detajuara për vazhdimin e vlefshmërisë se sistemeve të avionëve pa pilot të certifikuar dhe të përbërësve të tyre, si dhe për miratimin e organizatave dhe personelit të përfshirë në këto detyra që përafron Rregulloren Evropiane 2024/1107.

4. Kjo Rregullore nuk cenon kërkesat e sigurisë së informacionit dhe sigurisë kibernetike të përcaktuara në VKM nr. 411, datë 19.6.2024, "Për miratimin e Programit Kombëtar të Sigurisë së Aviacionit Civil", dhe në legjislacioni në fuqi për sigurinë kibernetike.

Neni 3

Përkufizimet

Për qëllimet e kësaj Rregulloreje, zbatohen përkufizimet e mëposhtme:

1. “Siguria e informacionit” nënkupton ruajtjen e konfidencialitetit, integritetit, autenticitetit dhe disponueshmërisë së rrjetit dhe sistemeve të informacionit;

2. “Ngjarje e sigurisë së informacionit” nënkupton një ndodhi të identifikuar të një sistemi, shërbimi ose gjendjeje rrjeti që tregon një shkelje të mundshme të politikës së sigurisë së informacionit ose dështimin e kontrolleve të sigurisë së informacionit, ose një situatë të panjohur më parë që mund të jetë e rëndësishme për sigurinë e informacionit;

3. “Incident” është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara ose të shërbimeve të ofruara apo të aksesueshme përmes rrjeteve dhe sistemeve të informacionit;

4. “Rreziku i sigurisë së informacionit” nënkupton rrezikun për operimet organizative të aviacionit civil, asetet, individët dhe organizatat e tjera, për shkak të potencialit të një ngjarjeje të sigurisë së informacionit. Rreziqet e sigurisë së informacionit shoqërohen me potencialin që kërcënimet të shfrytëzojnë dobësitë e një aseti informacioni ose një grupi asetesh informacioni;

5. “Kërcënim” nënkupton një shkelje të mundshme të sigurisë së informacionit që ekziston, kur ekziston një subjekt, rrethanë, veprim ose ngjarje që mund të shkaktojë dëm;

6. “Vulnerabilitet” nënkupton një defekt ose cenueshmëri në një aset ose një sistem, procedurë, projektim, zbatim, ose masa sigurie informacioni që mund të shfrytëzohen dhe që rezulton në një tejkalim, ose shkelje të politikës së sigurisë së informacionit.

Neni 4

Kërkesat për organizatat dhe autoritetet kompetente

1. Organizatat e përmendura në nenin 2, pika 1, duhet të jenë në përputhje me kërkesat e aneksit II (pjesa-IS.I.OR) të kësaj Rregulloreje.

2. Autoritetet kompetente të përmendura në nenin 2, pika 2, 3 dhe 3(a) duhet të jenë në përputhje me kërkesat e aneksit I (pjesa-IS.AR) të kësaj Rregulloreje.

Neni 5

Kërkesat që lindin nga legjislacioni tjetër kombëtar

1. Kur një organizatë e përmendur në nenin 2, pika 1, zbaton kërkesat e sigurisë të përcaktuara në përputhje me legjislacioni në fuqi për sigurinë kibernetike, që janë të barasvlershme me kërkesat e përcaktuara në këtë Rregullore, zbatimi i atyre kërkesave të sigurisë duhet të konsiderohet se përbën zbatim të kërkesave të përcaktuara në këtë Rregullore.

2. Kur një organizatë e përmendur në nenin 2, pika 1, është një operator ose një subjekt i referuar në programet kombëtare të sigurisë në operim të përcaktuara në përputhje me nenin 10 të udhëzimit nr. 26, datë 20.10.2010, “Mbi rregullat e përgjithshme në fushën e sigurisë së Aviacionit Civil”, kërkesat për sigurinë kibernetike të përfshira në VKM-në nr. 411, datë 19.6.2024, “Për miratimin e Programit Kombëtar të Sigurisë së Aviacionit Civil”, si dhe në aneksin e urdhrit të ministrit nr. 163, datë 26.3.2021, “Për përcaktimin e masave të detajuara për zbatimin e standardeve themelore të përbashkëta në fushën e sigurisë së aviacionit civil”, i ndryshuar, konsiderohen të barasvlershme me kërkesat e përcaktuara në këtë Rregullore, me përjashtim të pikës IS.I.OR.230 të aneksit II të kësaj Rregulloreje që do të respektohet si e tillë.

3. Ministri pas konsultimit me Autoritetin e Aviacionit Civil dhe Autoritetin përgjegjës për Sigurinë Kibernetike, mund të miratojë udhëzime për vlerësimin e ekuivalencës së kërkesave të përcaktuara në këtë Rregullore dhe rregullat kombëtare, në lidhje me masat për një nivel të lartë të sigurisë kibernetike.

Neni 6
Autoriteti kompetent

1. Autoriteti përgjegjës për certifikimin dhe mbikëqyrjen e zbatimit të kësaj Rregulloreje është:

a) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "a", Autoriteti i Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent në përputhje me aneksin II (pjesa-145) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra";

b) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "b", Autoriteti i Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent në përputhje me aneksin Vc (pjesa-CAMO) të urdhrit të ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra";

c) në lidhjet me organizatat e përmendura në nenin 2, pika 1, shkronja "c", Autoriteti i Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent në përputhje me aneksin III (pjesa-ORO) të urdhrit të ministrit nr. 80, datë 30.6.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative për operimet ajrore", i ndryshuar;

d) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronjat "d" deri "f", shkronja "c", Autoriteti i Aviacionit Civil, kur ai është përcaktuar si autoriteti kompetent në përputhje me aneksin VII (pjesa-ORA) të urdhrit të ministrit nr. 178, datë 20.12.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative, në lidhje me ekuipazhin ajror të aviacionit civil", i ndryshuar;

e) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "g", Autoriteti i Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent në përputhje me nenin 6, pika 2, të urdhrit të ministrit nr. 171, datë 11.11.2025, "Për miratimin e rregullores mbi përcaktimin e kërkesave teknike edhe procedurave administrative në lidhje me licencat dhe certifikatat e kontrollorëve të trafikut ajror";

f) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "h", Autoriteti i Aviacionit Civil kur ai është përcaktuar si autoriteti kompetent në përputhje me nenin 4, pika 1, të urdhrit të ministrit nr. 193, datë 6.10.2022, "Për miratimin e rregullores për përcaktimin e kërkesave të përbashkëta për ofruesit e shërbimeve të menaxhimit të trafikut ajror dhe të lundrimit ajror, si dhe funksionet e tjera të rrjetit të menaxhimit të trafikut ajror dhe mbikëqyrjen e tyre", i ndryshuar;

g) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "i", Autoriteti i Aviacionit Civil, kur ai është përcaktuar si autoriteti kompetent në përputhje me nenin 14, pika 1 ose pika 2, sipas rastit, të urdhrit të ministrit nr. 119, datë 29.9.2023, "Për miratimin e rregullores mbi kuadrin rregullator për hapësirën – U të hapësirës ajrore";

h) në lidhje me organizatat e përmendura në nenin 2, pika 1, shkronja "j", autoriteti kompetent i caktuar në përputhje me nenin 3, pika 1 të shtojcës II mbi rregulloren që përcakton kërkesat teknike dhe procedurat administrative për miratimin e organizatave të përfshira në projektimin ose prodhimin e sistemeve dhe përbërësve të menaxhimit të trafikut ajror/shërbimeve të lundrimit

ajror, të urdhrit të ministrit nr. 40, datë 12.3.2025, që përafron rregulloren zbatuese të Komisionit (BE) 2023/1769.

2. Në rast se legjislacioni kombëtar, për qëllimet e kësaj Rregulloreje, përcakton një entitet të pavarur dhe autonom për të përmbushur rolin dhe përgjegjësitë e caktuara të autoriteteve kompetente të përmendura në pikën 1, masat e koordinimit do të vendosen ndërmjet atij entiteti dhe autoriteteve kompetente, e përmendura në pikën 1, për të siguruar mbikëqyrje efektive të të gjitha kërkesave që duhet të përmbushen nga organizatat.

Neni 7

Dorëzimi i informacionit përkatës pranë Autoritetit përgjegjës për sigurinë kibernetike

Autoritetet kompetente sipas kësaj Rregulloreje do të informojnë, pa vonesa të panevojshme, pikën e vetme të kontaktit të caktuar në përputhje me legjislacioni në fuqi për sigurinë kibernetike për çdo informacion përkatës të përfshirë në njoftimet e paraqitura në përputhje me pikën IS.I.OR.230 të aneksit II të kësaj Rregulloreje dhe pikës IS.D.OR.230 të aneksit I të Rregullores për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, "Për miratimin e kërkesave thelbësore në fushën e aviacionit civil", i ndryshuar, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhrit të ministrit nr. 57, datë 13.3.2024, dhe urdhrit të ministrit nr. 170, datë 13.9.2022, i ndryshuar, që përafron rregulloren e deleguar të Komisionit (BE) 2022/1645, sipas shtojcës I të këtij urdhri, nga operatorët e infrastrukturave të informacionit të identifikuar në përputhje me legjislacioni në fuqi për sigurinë kibernetike.

ANEKSI I

SIGURIA E INFORMACIONIT – KËRKESAT E AUTORITETIT

[PJESA-IS.AR]

IS.AR.100	Fushëveprimi
IS.AR.200	Sistemi i menaxhimit të sigurisë së informacionit (ISMS)
IS.AR.205	Vlerësimi i rrezikut të sigurisë së informacionit
IS.AR.210	Trajtimi i rrezikut të sigurisë së informacionit
IS.AR.215	Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi
IS.AR.220	Kontraktimi i aktiviteteve të menaxhimit të sigurisë së informacionit
IS.AR.225	Kërkesat e personelit
IS.AR.230	Ruajtja e të dhënave
IS.AR.235	Përmirësimi i vazhdueshëm

IS.AR.100 Fushëveprimi

Kjo pjesë përcakton kërkesat për menaxhimin që duhet të plotësojnë autoritetet kompetente të referuara në nenin 2, pika 2 të kësaj Rregulloreje.

Kërkesat që duhet të plotësojnë këto autoritete kompetente për kryerjen e aktiviteteve të tyre të certifikimit, mbikëqyrjes dhe zbatimit përmbahen në rregulloret e përmendura në nenin 2, pika 1, të kësaj Rregulloreje dhe në nenin 2 të Rregullores për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, "Për miratimin e kërkesave thelbësore në fushën e aviacionit civil", i ndryshuar, në lidhje me kërkesat për menaxhimin e

rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhrit të ministrit nr. 57, datë 13.3.2024, dhe urdhrit të ministrit nr. 170, datë 13.9.2022, i ndryshuar, që përafron rregulloren e deleguar të Komisionit (BE) 2022/1645, sipas shtojcës I të këtij urdhri.

IS.AR.200 Sistemi i menaxhimit të sigurisë së informacionit (ISMS)

a) Për të arritur objektivat e përcaktuar në nenin 1, autoriteti kompetent ngre, zbaton dhe mirëmban një sistem të menaxhimit të sigurisë së informacionit (ISMS), i cili siguron që autoriteti kompetent:

1. vendos një politikë për sigurinë e informacionit që përcakton parimet e përgjithshme të autoritetit kompetent në lidhje me ndikimin e mundshëm të rreziqeve të sigurisë së informacionit në sigurinë në operim;

2. identifikon dhe rishikon rreziqet e sigurisë së informacionit në përputhje me pikën IS.AR.205;

3. përcakton dhe zbaton masat e trajtimit të rrezikut të sigurisë së informacionit në përputhje me pikën IS.AR.210;

4. përcakton dhe zbaton, në përputhje me pikën IS.AR.215, masat e kërkuara për zbulimin e ngjarjeve të sigurisë së informacionit, identifikon ato që konsiderohen si incidente me një ndikim të mundshëm në sigurinë në operim të aviacionit, dhe u përgjigjet dhe merret me rikuperimin pas këtyre incidenteve të sigurisë së informacionit;

5. përputhet me kërkesat e përfshira në pikën IS.AR.220, kur kontrakton ndonjë pjesë të aktiviteteve të përshkruara në pikën IS.AR.200 me organizata të tjera;

6. përputhet me kërkesat e personelit të përfshira në pikën IS.AR.225;

7. përputhet me kërkesat e mbajtjes së të dhënave të përfshira në pikën IS.AR.230;

8. monitoron përputhshmërinë e vetë organizatës së tij me kërkesat e kësaj Rregulloreje dhe jep komente mbi gjetjet për personin e përmendur në pikën IS.AR.225 (a) për të siguruar zbatimin efektiv të veprimeve korrigjuese;

9. mbron konfidencialitetin e çdo informacioni që autoriteti kompetent mund të ketë në lidhje me organizatat që i nënshtrohen mbikëqyrjes së tij dhe informacionin e marrë nëpërmjet skemave të raportimit të jashtëm të organizatës, të përcaktuara në përputhje me pikën IS.I.OR.230 të aneksit II (pjesa-IS.I.OR) të kësaj Rregulloreje dhe pikës IS.D.OR.230 të aneksit (pjesa-IS.D.OR) të Rregullores për përcaktimin e rregullave për zbatimin e vendimit të Këshillit të Ministrave nr. 1095, datë 24.12.2020, "Për miratimin e kërkesave thelbësore në fushën e aviacionit civil", të ndryshuar, në lidhje me kërkesat për menaxhimin e rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim për organizatat e mbuluara nga urdhrit të ministrit nr. 57, datë 13.3.2024 dhe urdhrit të ministrit nr. 170, datë 13.9.2022, i ndryshuar, që përafron Rregulloren e Deleguar të Komisionit (BE) 2022/1645, sipas shtojcës I të këtij urdhri.

10. kur të jetë e zbatueshme, njofton Agjencinë për ndryshimet që ndikojnë në aftësinë e autoritetit kompetent për të kryer detyrat e tij dhe për të mbuluar përgjegjësitë e tij siç janë përcaktuar në këtë Rregullore;

11. përcakton dhe zbaton procedurat për të ndarë sipas rastit dhe në mënyrë praktike dhe të përpiktë informacionin përkatës për të ndihmuar autoritetet kompetente dhe agjencitë e tjera, si dhe organizatat që i nënshtrohen kësaj Rregulloreje për të kryer vlerësime efektive të rrezikut të sigurisë në lidhje me aktivitetet e tyre.

b) Për të përmbushur vazhdimisht kërkesat e përmendura në nenin 1, autoriteti kompetent zbaton një proces përmirësimi të vazhdueshëm në përputhje me pikën IS.AR.235.

c) Autoriteti kompetent dokumenton të gjitha proceset, procedurat, rolet dhe përgjegjësitë kyçe që kërkohen për të qenë në përputhje me pikën IS.AR.200(a) dhe vendos një proces për ndryshimin e këtij dokumentacioni.

d) Proceset, procedurat, rolet dhe përgjegjësitë e përcaktuara nga autoriteti kompetent në zbatim të pikës IS.AR.200(a) përputhen me natyrën dhe kompleksitetin e aktiviteteve të tij, bazuar në një vlerësim të rreziqeve të sigurisë së informacionit të qenësishme për ato aktivitete, dhe mund të integrohen brenda sistemeve të tjera ekzistuese të menaxhimit të zbatuara tashmë nga autoriteti kompetent.

IS.AR.205 Vlerësimi i rrezikut të sigurisë së informacionit

a) Autoriteti kompetent identifikon të gjitha elementet e organizatës së tij që mund të ekspozohen ndaj rreziqeve të sigurisë së informacionit. Kjo përfshin:

1. aktivitetet, objektet dhe burimet e autoritetit kompetent, si dhe shërbimet që autoriteti kompetent operon, ofron, merr ose mirëmban;

2. pajisjet, sistemet, të dhënat dhe informacionet që ndikojnë në funksionimin e elementeve të përmendura në pikën 1.

b) Autoriteti kompetent identifikon ndërlidhjet që organizata e tij ka me organizata të tjera dhe që mund të rezultojë në ekspozimin e ndërsjellë ndaj rreziqeve të sigurisë së informacionit.

c) Për elementet dhe ndërlidhjet e përmendura në shkronjat "a" dhe "b", autoriteti kompetent identifikon rreziqet e sigurisë së informacionit që mund të kenë një ndikim të mundshëm në sigurinë në operim.

Për çdo rrezik të identifikuar, autoriteti kompetent duhet:

1. të caktojë një nivel rreziku sipas një klasifikimi të paracaktuar të vendosur nga autoriteti kompetent;

2. të lidhë çdo rrezik dhe nivelin e tij me elementin ose ndërlidhjen përkatëse të identifikuar në përputhje me shkronjat "a" dhe "b".

Klasifikimi i paracaktuar i referuar në pikën 1 merr parasysh potencialin e shfaqjes së skenarit kërcënues dhe ashpërsinë e pasojave të tij mbi sigurinë në operim. Nëpërmjet këtij klasifikimi dhe duke marrë parasysh nëse autoriteti kompetent ka një proces të strukturuar dhe të përsëritshëm të menaxhimit të rrezikut për operimet, autoriteti kompetent do të jetë në gjendje të përcaktojë nëse rreziku është i pranueshëm ose duhet të trajtohet në përputhje me pikën IS.AR.210.

Për të lehtësuar krahasueshmërinë e ndërsjellë të vlerësimeve të rreziqeve, caktimi i nivelit të rrezikut për pikën 1 do të marrë parasysh informacionin përkatës të marrë në koordinim me organizatat e përmendura në shkronjën "b".

d) Autoriteti kompetent rishikon dhe përditëson vlerësimin e rrezikut të kryer në përputhje me shkronjat "a", "b" dhe "c" në cilindo nga rastet e mëposhtme:

1. ka një ndryshim në elementet që u nënshtrohen rreziqeve të sigurisë së informacionit;

2. ka një ndryshim në lidhjet ndërmjet organizatës së autoritetit kompetent dhe organizatave të tjera, ose në rreziqet e komunikuara nga organizatat e tjera;

3. ka një ndryshim në informacionin ose njohuritë e përdorura për identifikimin, analizën dhe klasifikimin e rreziqeve;

4. ka mësime të nxjerra nga analiza e incidenteve të sigurisë së informacionit.

IS.AR.210 Trajtimi i rrezikut të sigurisë së informacionit

a) Autoriteti kompetent merr masa për të trajtuar rreziqet e papranueshme të identifikuara në përputhje me pikën IS.AR.205, i zbaton ato në kohën e duhur dhe kontrollon efektivitetin e tyre të vazhdueshëm. Këto masa i mundësojnë autoritetit kompetent, që:

1. të kontrollojë rrethanat që ndikojnë në shfaqjen efektive të skenarit kërcënues;

2. të zvogëlojë pasojat për sigurinë në operim që lidhen me shfaqjen e skenarit kërcënues;

3. të shmangë rreziqet.

Këto masa nuk sjellin ndonjë rrezik të ri të mundshëm të papranueshëm për sigurinë në operim.

b) Personi i përmendur në pikën IS.AR.225(a) dhe stafi tjetër i prekur i autoritetit kompetent njoftohen për rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.AR.205, skenarët kërcënues përkatës dhe masat që duhen zbatuar.

Autoriteti kompetent informon gjithashtu organizatat me të cilat ka një ndërlidhje në përputhje me pikën IS.AR.205 (b) për çdo rrezik të njohur ndërmjet autoritetit kompetent dhe organizatës.

IS.AR.215 Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi

a) Bazuar në rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.AR.205 dhe rezultatin e trajtimit të rrezikut të kryer në përputhje me pikën IS.AR.210, autoriteti kompetent zbaton masa për zbulimin e ngjarjeve që tregojnë potencialin e shfaqjes së rreziqeve të papranueshme dhe që mund të kenë një ndikim të mundshëm në sigurinë në operim. Këto masa zbulimi i mundësojnë autoritetit kompetent, që:

1. të identifikojë devijimet nga linjat bazë të paracaktuara të performancës funksionale;

2. të lëshojë paralajmërimet për të aktivizuar masat e duhura të reagimit, në rast të ndonjë devijimi.

b) Autoriteti kompetent zbaton masa për t'iu përgjigjur të gjitha kushteve të ngjarjeve të identifikuara, në përputhje me shkronjën "a", që mund të shndërrohen ose që janë shndërruar në një incident të sigurisë së informacionit. Këto masa reagimi i mundësojnë autoritetit kompetent, që:

1. të fillojë reagimin e organizatës së tij ndaj paralajmërimeve të përmendura në pikën (a)(2), duke aktivizuar burimet e paracaktuara dhe rendin e veprimeve;

2. të përmbajë përhapjen e një sulmi dhe të shmangë shfaqjen e plotë të një skenari kërcënues;

3. të kontrollojë mënyrën e mosfunksionimit të elementeve të prekura, të përcaktuara në pikën IS.AR.205(a).

c) Autoriteti kompetent zbaton masat që synojnë rikuperimin mbas incidenteve të sigurisë së informacionit, duke përfshirë masat emergjente, nëse është e nevojshme. Këto masa rikuperimi i mundësojnë autoritetit kompetent, që:

1. të eliminojë gjendjen që shkaktoi incidentin, ose ta kufizojë atë në një nivel të tolerueshëm;

2. të rivendosë një gjendje të sigurt të elementeve të prekura, të përcaktuara në pikën IS.AR.205(a) brenda një kohe rikuperimi të përcaktuar më parë nga organizata e tij.

IS.AR.220 Kontraktimi i veprimtarive të menaxhimit të sigurisë së informacionit

Autoriteti kompetent siguron që gjatë kontraktimit të ndonjë pjese të aktiviteteve të përmendura në pikën IS.AR.200 me organizata të tjera, aktivitetet e kontraktuara janë në përputhje me kërkesat e kësaj Rregulloreje dhe organizata e kontraktuar punon nën mbikëqyrjen e tij. Autoriteti kompetent siguron që rreziqet që lidhen me aktivitetet e kontraktuara të menaxhohen, siç duhet.

IS.AR.225 Kërkesat e personelit

Autoriteti kompetent do të:

a) ketë një person që ka autoritetin për të krijimin dhe mbarëvajtjen e strukturave organizative, politikave, proceseve dhe procedurave të nevojshme për zbatimin e kësaj Rregulloreje.

Ky person duhet:

1. të ketë autoritet për t'u qasur plotësisht te burimet e nevojshme për autoritetin kompetent për të kryer të gjitha detyrat e kërkuara nga kjo Rregullore;

2. të zotërojë delegimin e kompetencave të nevojshme për të kryer detyrat e caktuara;

b) ketë një proces për t'u siguruar që ai ka staf të mjaftueshëm në detyrë për të kryer aktivitetet e mbuluara nga ky aneks;

c) ketë një proces për t'u siguruar që personeli i përmendur në shkronjën "b" të ketë kompetencën e nevojshme për të kryer detyrat e tyre;

d) ketë një proces për t'u siguruar që personeli të pranojë përgjegjësitë që lidhen me rolet dhe detyrat e caktuara;

e) sigurohet që identiteti dhe besueshmëria e personelit, të cilët kanë akses në sistemet e informacionit dhe të dhënat që u nënshtrohen kërkesave të kësaj Rregulloreje janë përcaktuar siç duhet.

IS.AR.230 Ruajtja e të dhënave

a) Autoriteti kompetent duhet të ruajë të dhënat për aktivitetet e tij të menaxhimit të sigurisë së informacionit.

1. Autoriteti kompetent duhet të sigurohet që të dhënat e mëposhtme të jenë të arkivuara dhe të gjurmueshme:

i. kontratat për aktivitetet e përmendura në pikën IS.AR.200(a)(5);

ii. regjistrimet e proceseve kryesore të referuara në pikën IS.AR.200(d);

iii. të dhënat e rreziqeve të identifikuara në vlerësimin e rrezikut të përmendur në pikën IS.AR.205 së bashku me masat shoqëruese të trajtimit të rrezikut të përmendura në pikën IS.AR.210;

iv. të dhënat e ngjarjeve të sigurisë së informacionit të cilat mund të kenë nevojë të rivlerësohen për të zbuluar incidente ose cenueshmëri të pazbuluara të sigurisë së informacionit.

2. Të dhënat e përmendura në pikën (1)(i) ruhen të paktën deri në 5 vjet pas ndryshimit ose përfundimit të kontratës.

3. Të dhënat e përmendura në pikën (1)(ii) dhe (iii) ruhen të paktën për një periudhë prej 5 vjetësh.

4. Të dhënat e përmendura në pikën (1)(iv) ruhen derisa ato ngjarje të sigurisë së informacionit të rivlerësohen në përputhje me një periodicitet të përcaktuar në një procedurë të vendosur nga Autoriteti kompetent.

b) Autoriteti kompetent duhet të ruajë të dhëna për kualifikimin dhe përvojën e personelit të tij të përfshirë në aktivitetet e menaxhimit të sigurisë së informacionit.

1. Të dhënat e kualifikimit dhe përvojës së personelit ruhen për aq kohë sa personi punon për autoritetin kompetent dhe për të paktën 3 vjet, pasi personi të jetë larguar nga autoriteti kompetent.

2. Anëtarëve të stafit, me kërkesën e tyre, u jepet akses në të dhënat e tyre individuale. Gjithashtu, me kërkesën e tyre, autoriteti kompetent u siguron atyre një kopje të të dhënave të tyre individuale pas largimit nga autoriteti kompetent.

c) Formati i të dhënave duhet të specifikohet në procedurat e autoritetit kompetent.

d) Të dhënat ruhen në një mënyrë që siguron mbrojtje nga dëmtimi, ndryshimi dhe vjedhja, me informacionin që identifikohet, kur kërkohet, sipas nivelit të klasifikimit të sigurisë. Autoriteti kompetent siguron që të dhënat të ruhen, duke përdorur mjete për të siguruar integritetin, autenticitetin dhe aksesin e autorizuar.

IS.AR.235 Përmirësimi i vazhdueshëm

a) Autoriteti kompetent vlerëson, duke përdorur tregues të përshtatshëm të performancës, efektivitetin dhe pjekurinë e ISMS-së së tij. Vlerësimi kryhet mbi një bazë kalendarike të përcaktuar nga autoriteti kompetent ose pas një incidenti të sigurisë së informacionit.

b) Nëse konstatohen mangësi pas vlerësimit të kryer në përputhje me shkronjën "a", autoriteti kompetent merr masat e nevojshme të përmirësimit për të siguruar që ISMS-ja të vazhdojë të jetë

në përputhje me kërkesat në fuqi dhe të mbajë rreziqet e sigurisë së informacionit në një nivel të pranueshëm. Përveç kësaj, autoriteti kompetent rivlerëson ato elemente të ISMS-së të prekura nga masat e miratuara.

ANEKSI II
SIGURIA E INFORMACIONIT – KËRKESAT E ORGANIZATËS

[PJESA-IS.I.OR]

IS.I.OR.100	Fushëveprimi
IS.I.OR.200	Sistemi i menaxhimit të sigurisë së informacionit (ISMS)
IS.I.OR.205	Vlerësimi i rrezikut të sigurisë së informacionit
IS.I.OR.210	Trajtimi i rrezikut të sigurisë së informacionit
IS.I.OR.215	Skema e raportimit të brendshëm të sigurisë së informacionit
IS.I.OR.220	Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi
IS.I.OR.225	Përgjigje ndaj gjetjeve të njoftuara nga autoriteti kompetent
IS.I.OR.230	Skema e raportimit të jashtëm të sigurisë së informacionit
IS.I.OR.235	Kontraktimi i aktiviteteve të menaxhimit të sigurisë së informacionit
IS.I.OR.240	Kërkesat e personelit
IS.I.OR.245	Ruajtja e të dhënave
IS.I.OR.250	Manuali i menaxhimit të sigurisë së informacionit (ISMM)
IS.I.OR.255	Ndryshime në sistemin e menaxhimit të sigurisë së informacionit
IS.I.OR.260	Përmirësimi i vazhdueshëm

IS.I.OR.100 Fushëveprimi

Kjo pjesë përcakton kërkesat që duhet të plotësojnë organizatat e përmendura në nenin 2, pika 1 të kësaj Rregulloreje.

IS.I.OR.200 Sistemi i menaxhimit të sigurisë së informacionit (ISMS)

a) Për të arritur objektivat e përcaktuar në nenin 1, organizata duhet të krijojë, zbatojë dhe mirëmbajë një sistem të menaxhimit të sigurisë së informacionit (ISMS), i cili siguron që organizata:

1. vendos një politikë për sigurinë e informacionit duke përcaktuar parimet e përgjithshme të organizatës në lidhje me ndikimin e mundshëm të rreziqeve të sigurisë së informacionit në sigurinë në operim;

2. identifikon dhe rishikon rreziqet e sigurisë së informacionit në përputhje me pikën IS.I.OR.205;

3. përcakton dhe zbaton masat e trajtimit të rrezikut të sigurisë së informacionit, në përputhje me pikën IS.I.OR.210;

4. zbaton një skemë raportimi të brendshëm të sigurisë së informacionit në përputhje me pikën IS.I.OR.215;

5. përcakton dhe zbaton, në përputhje me pikën IS.I.OR.220, masat e nevojshme për zbulimin e ngjarjeve të sigurisë së informacionit, identifikon ato ngjarje që konsiderohen si incidente me një ndikim të mundshëm në sigurinë në operim, me përjashtim të rasteve të lejuara nga pika IS.I.OR.205(e) dhe u përgjigjet dhe merr masa për t'iu përgjigjur këtyre incidenteve dhe për të rikuperuar pas tyre;

6. zbaton masat që janë njoftuar nga autoriteti kompetent si reagim i menjëhershëm ndaj një incidenti ose cenueshmërie të sigurisë së informacionit me ndikim në sigurinë në operim;

7. merr masat e duhura, në përputhje me pikën IS.I.OR.225, për të adresuar gjetjet e njoftuara nga autoriteti kompetent;

8. zbaton një skemë raportimi të jashtëm në përputhje me pikën IS.I.OR.230 për t'i dhënë mundësi autoritetit kompetent të ndërmarrë veprimet e duhura;

9. përputhet me kërkesat e përfshira në pikën IS.I.OR.235, kur kontrakton ndonjë pjesë të aktiviteteve të përmendura në pikën IS.I.OR.200 me organizata të tjera;

10. përputhet me kërkesat e personelit të përcaktuara në pikën IS.I.OR.240;

11. përputhet me kërkesat e ruajtjes së të dhënave të përcaktuara në pikën IS.I.OR.245;

12. monitoron përputhshmërinë e organizatës me kërkesat e kësaj Rregulloreje dhe jep komente mbi gjetjet te menaxheri përgjegjës për të siguruar zbatimin efektiv të veprimeve korrigjuese;

13. mbron, pa cenuar kërkesat në fuqi të raportimit të incidentit, konfidencialitetin e çdo informacioni që organizata mund të ketë marrë nga organizata të tjera, sipas nivelit të saj të ndjeshmërisë.

b) Për të përmbushur vazhdimisht kërkesat e referuara në nenin 1, organizata zbaton një proces përmirësimi të vazhdueshëm në përputhje me pikën IS.I.OR.260.

c) Organizata dokumenton, në përputhje me pikën IS.I.OR.250, të gjitha proceset kryesore, procedurat, rolet dhe përgjegjësitë e kërkuara për të qenë në përputhje me pikën IS.I.OR.200(a) dhe krijon një proces për ndryshimin e këtij dokumentacioni. Ndryshimet në këto procese, procedura, role dhe përgjegjësi menaxhohen në përputhje me pikën IS.I.OR.255.

d) Proceset, procedurat, rolet dhe përgjegjësitë e përcaktuara nga autoriteti kompetent në zbatim të pikës IS.AR.200(a) përputhen me natyrën dhe kompleksitetin e aktiviteteve të tij, bazuar në një vlerësim të rreziqeve të sigurisë së informacionit të qenësishme për ato aktivitete, dhe mund të integrohen brenda sistemeve të tjera ekzistuese të menaxhimit të zbatuara tashmë nga autoriteti kompetent.

e) Pa cenuar detyrimin për të përmbushur kërkesat e raportimit të përcaktuara në urdhrin e ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë" dhe kërkesat e përcaktuara në pikën IS.I.OR.200 (a)(13), organizata mund të lejohet nga autoriteti kompetent që të mos zbatojë kërkesat e përmendura në shkronjat "a" deri në (d) dhe kërkesat përkatëse të përfshira në pikat IS.I.OR.205 deri IS.I.OR.260, nëse tregon në mënyrë të kënaqshme për atë autoritet se aktivitetet, objektet dhe burimet e saj, si dhe shërbimet që ajo operon, ofron, merr dhe mirëmban, nuk paraqesin ndonjë rrezik sigurie informacioni me një ndikim të mundshëm në sigurinë në operim, as për veten dhe as për organizatat e tjera. Miratimi bazohet në një vlerësim të dokumentuar të rrezikut të sigurisë së informacionit të kryer nga organizata ose një palë e tretë në përputhje me pikën IS.I.OR.205 dhe të rishikuar dhe miratuar nga autoriteti i saj kompetent.

Vlefshmëria e vazhdueshme e atij miratimi rishikohet nga autoriteti kompetent pas ciklit të zbatueshëm të auditimit të mbikëqyrjes dhe sa herë që zbatohen ndryshime në fushën e punës së organizatës.

IS.I.OR.205 Vlerësimi i rrezikut të sigurisë së informacionit

a) Organizata duhet të identifikojë të gjitha elementet e saj që mund të ekspozohen ndaj rreziqeve të sigurisë së informacionit. Kjo përfshin:

1. aktivitetet, objektet dhe burimet e organizatës, si dhe shërbimet që organizata operon, ofron, merr ose mirëmban;

2. pajisjet, sistemet, të dhënat dhe informacionet që ndikojnë në funksionimin e elementeve të renditura në pikën 1.

b) Organizata duhet të identifikojë ndërlidhjet që ka me organizatat e tjera dhe që mund të rezultojë në ekspozimin e ndërsjellë ndaj rreziqeve të sigurisë së informacionit.

c) Për elementet dhe ndërlidhjet e përmendura në shkronjat "a" dhe "b", organizata identifikon rreziqet e sigurisë së informacionit që mund të kenë një ndikim të mundshëm në sigurinë në operim. Për çdo rrezik të identifikuar, organizata duhet:

1. të caktojë një nivel rreziku sipas një klasifikimi të paracaktuar të vendosur nga organizata;

2. të lidhë çdo rrezik dhe nivelin e tij me elementin ose ndërlidhjen përkatëse të identifikuar në përputhje me shkronjat "a" dhe "b".

Klasifikimi i paracaktuar i referuar në pikën 1 merr parasysh potencialin e shfaqjes së skenarit kërcënues dhe ashpërsinë e pasojave të tij mbi sigurinë në operim. Nëpërmjet këtij klasifikimi, dhe duke marrë parasysh nëse organizata ka një proces të strukturuar dhe të përsëritshëm të menaxhimit të rrezikut për operacionet, organizata është në gjendje të përcaktojë nëse rreziku është i pranueshëm ose duhet të trajtohet në përputhje me pikën IS.AR.210.

Për të lehtësuar krahasueshmërinë e ndërsjellë të vlerësimeve të rreziqeve, caktimi i nivelit të rrezikut për pikën 1 do të marrë parasysh informacionin përkatës të marrë në koordinim me organizatat e përmendura në shkronjën "b".

d) Organizata rishikon dhe përditëson vlerësimin e rrezikut të kryer në përputhje me shkronjat "a", (b) dhe, sipas rastit, shkronjat "c" ose "e" në cilindo nga rastet e mëposhtme:

1. ka një ndryshim në elementet që u nënshtrohen rreziqeve të sigurisë së informacionit;

2. ka një ndryshim në ndërlidhjet ndërmjet organizatës së autoritetit kompetent dhe organizatave të tjera, ose në rreziqet e komunikuara nga organizatat e tjera;

3. ka një ndryshim në informacionin ose njohuritë e përdorura për identifikimin, analizën dhe klasifikimin e rreziqeve;

4. ka mësime të nxjerra nga analiza e incidenteve të sigurisë së informacionit.

e) Me përjashtim nga shkronja "c", organizatave që u kërkohet të pajtohen me nënpjesën C të aneksit III (pjesa-ATM/ANS.OR) të urdhrit të ministrit nr. 193, datë 6.10.2022, "Për miratimin e rregullores për përcaktimin e kërkesave të përbashkëta për ofruesit e shërbimeve të menaxhimit të trafikut ajror dhe të lundrimit ajror, si dhe funksionet e tjera të rrjetit të menaxhimit të trafikut ajror dhe mbikëqyrjen e tyre", të ndryshuar, do të zëvendësojnë analizën e ndikimit në sigurinë në operim me një analizë të ndikimit në shërbimet e tyre sipas vlerësimit të mbështetjes së sigurisë në operim që kërkohet nga pika ATM/ANS.OR.C.005. Ky vlerësim mbështetës i sigurisë në operim do t'u vihet në dispozicion ofruesve të shërbimeve të trafikut ajror të cilëve ata u ofrojnë shërbime dhe ata ofrues të shërbimeve të trafikut ajror do të jenë përgjegjës për vlerësimin e ndikimit në sigurinë e aviacionit.

IS.I.OR.210 Trajtimi i rrezikut të sigurisë së informacionit

a) Organizata merr masa për të trajtuar rreziqet e papranueshme të identifikuara në përputhje me pikën IS.OR.205, i zbaton ato në kohën e duhur dhe kontrollon efektivitetin e tyre të vazhdueshëm. Këto masa i mundësojnë autoritetit kompetent, që:

1. të kontrollojë rrethanat që ndikojnë në shfaqjen efektive të skenarit kërcënues;

2. të zvogëlojë pasojat për sigurinë në operim që lidhen me shfaqjen e skenarit kërcënues;

3. të shmangë rreziqet.

Këto masa nuk sjellin ndonjë rrezik të ri të mundshëm të papranueshëm për sigurinë në operim.

b) Personi i përmendur në pikën IS.I.OR.225 (a) dhe (b) dhe stafi tjetër i prekur i autoritetit kompetent njoftohen për rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.OR.205, skenarët kërcënues përkatës dhe masat që duhen zbatuar.

Organizata informon, gjithashtu, organizatat me të cilat ka një ndërlidhje në përputhje me pikën IS.OR.205 (b) për çdo rrezik të njohur ndërmjet dy organizatave.

IS.I.OR.215 Skema e raportimit të brendshëm të sigurisë së informacionit

a) Organizata krijon një skemë të brendshme raportimi për të mundësuar mbledhjen dhe vlerësimin e ngjarjeve të sigurisë së informacionit, duke përfshirë ato që raportohen në përputhje me pikën IS.I.OR.230.

b) Kjo skemë dhe procesi i përmendur në pikën IS.I.OR.220 i mundësojnë organizatës, që:

1. të identifikojë se cilat nga ngjarjet e raportuara në përputhje me shkronjën "a" konsiderohen si incidente ose cenueshmëri të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim;

2. të identifikojë shkaqet dhe faktorët që ndikojnë në incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën 1, dhe t'i trajtojë ato si pjesë e procesit të menaxhimit të rrezikut të sigurisë së informacionit në përputhje me pikat IS.I.OR.205 dhe IS.I.OR.220;

3. të sigurojë një vlerësim të të gjithë informacionit përkatës të njohur, në lidhje me incidentet dhe cenueshmëritë e sigurisë së informacionit të identifikuara në përputhje me pikën 1;

4. të sigurojë zbatimin e një metode për shpërndarjen e brendshme të informacionit sipas nevojës;

c) Çdo organizate të kontraktuar, e cila mund ta ekspozojë organizatën ndaj rreziqeve të sigurisë së informacionit me një ndikim të mundshëm në sigurinë në operim do t'i kërkohet të raportojë ngjarjet e sigurisë së informacionit tek organizata. Këto raporte dorëzohen duke përdorur procedurat e përcaktuara në marrëveshjet specifike kontraktuale dhe vlerësohen në përputhje me shkronjën "b".

d) Organizata bashkëpunon në hetime me çdo organizatë tjetër që ka një kontribut të rëndësishëm në sigurinë e informacionit të aktiviteteve të saj.

e) Organizata mund ta integrojë atë skemë raportimi me skema të tjera raportimi që ajo ka zbatuar tashmë.

IS.I.OR.220 Incidentet e sigurisë së informacionit – zbulimi, reagimi dhe rikuperimi

a) Bazuar në rezultatin e vlerësimit të rrezikut të kryer në përputhje me pikën IS.AR.205 dhe rezultatin e trajtimit të rrezikut të kryer në përputhje me pikën IS.AR.210, organizata do të zbatojë masa për zbulimin e ngjarjeve që tregojnë potencialin e shfaqjes së rreziqeve të papranueshme dhe që mund të kenë një ndikim të mundshëm në sigurinë në operim. Këto masa zbulimi i mundësojnë autoritetit kompetent, që:

1. të identifikojë devijimet nga linjat bazë të paracaktuara të performancës funksionale;

2. të lëshojë paralajmërimet për të aktivizuar masat e duhura të reagimit, në rast të ndonjë devijimi.

b) Organizata zbaton masa për t'iu përgjigjur të gjitha kushteve të ngjarjeve të identifikuara në përputhje me shkronjën "a" që mund të shndërrohen ose që janë shndërruar në një incident të sigurisë së informacionit. Këto masa reagimi i mundësojnë organizatës, që:

1. të fillojë reagimin ndaj paralajmërimeve të përmendura në pikën (a)(2), duke aktivizuar burimet e paracaktuara dhe rendin e veprimeve;

2. të përmbajë përhapjen e një sulmi dhe të shmangë shfaqjen e plotë të një skenari kërcënues;

3. të kontrollojë mënyrën e mosfunksionimit të elementeve të prekura, të përcaktuara në pikën IS.I.OR.205(a).

c) Organizata zbaton masat që synojnë rikuperimin mbas incidenteve të sigurisë së informacionit, duke përfshirë masat emergjente, nëse është e nevojshme. Këto masa rikuperimi i mundësojnë organizatës, që:

1. të eliminojë gjendjen që shkaktoi incidentin, ose ta kufizojë atë në një nivel të tolerueshëm;

2. të rivendosë një gjendje të sigurt të elementeve të prekura, të përcaktuara në pikën IS.I.OR.205(a) brenda një kohe rikuperimi të përcaktuar më parë nga organizata e saj.

IS.I.OR.225 Përgjigje ndaj gjetjeve të njoftuara nga autoriteti kompetent

a) Pas marrjes së njoftimit për gjetjet e dorëzuar nga autoriteti kompetent, organizata duhet:

1. të identifikojë shkakun ose shkaqet rrënjësore dhe faktorët që ndikojnë në mospërputhje;

2. të përcaktojë një plan veprimi korrigjues;

3. të vërtetojë korrigjimin e mospërputhjes në mënyrë të kënaqshme për autoritetin kompetent.

b) Veprimet e përmendura në shkronjën "a" kryhen brenda periudhës së rënë dakord me autoritetin kompetent.

IS.I.OR.230 Skema e raportimit të jashtëm të sigurisë së informacionit

a) Organizata zbaton një sistem raportimi të sigurisë së informacionit që përputhet me kërkesat e përcaktuara në urdhrin e ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë" dhe çdo ndryshim të tij, nëse kjo Rregullore është e zbatueshme për organizatën.

b) Pa cenuar detyrimet e urdhrit të ministrit nr. 89, datë 5.5.2022, "Për miratimin e rregullores për raportimin dhe ndjekjen e ngjarjeve në aviacionin civil në Republikën e Shqipërisë", organizata duhet të sigurojë që çdo incident ose cenueshmëri e sigurisë së informacionit, që mund të përfaqësojë një rrezik të rëndësishëm për sigurinë në operim, t'i raportohet autoritetit të saj kompetent. Për më tepër:

1. Kur një incident ose cenueshmëri e tillë prek një avion ose sistem ose komponent përkatës, organizata duhet t'ia raportojë, gjithashtu, mbajtësit të miratimit të projektimit;

2. Kur një incident ose cenueshmëri e tillë prek një sistem ose përbërës të përdorur nga organizata, organizata duhet t'ia raportojë atë organizatës përgjegjëse për projektimin e sistemit, ose përbërësit.

c) Organizata duhet të raportojë situatat e përmendura në shkronjën "b", si më poshtë:

1. një njoftim i dorëzohet autoritetit kompetent dhe, sipas rastit, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit ose përbërësit, sapo organizata të vihet në dijeni për situatën;

2. një raport i dorëzohet autoritetit kompetent dhe, sipas rastit, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit, ose përbërësit, sa më shpejt të jetë e mundur, por jo më shumë se 72 orë nga koha kur organizata vihet në dijeni të situatës, përveç rasteve kur rrethanat e jashtëzakonshme e pengojnë këtë.

Raporti bëhet në formën e përcaktuar nga autoriteti kompetent dhe përmban të gjithë informacionin përkatës për situatën e njohur për organizatën;

3. një raport pasues i dorëzohet autoritetit kompetent dhe, sipas rastit, mbajtësit të miratimit të projektimit ose organizatës përgjegjëse për projektimin e sistemit, ose përbërësit, duke ofruar detaje të veprimeve që organizata ka ndërmarrë, ose synon të ndërmarrë për të rikuperuar pas incidentit dhe veprimet që synon të ndërmarrë për të parandaluar incidente të ngjashme të sigurisë së informacionit në të ardhmen.

Raporti pasues dorëzohet sapo të jenë identifikuar këto veprime dhe përgatitet në formën e përcaktuar nga autoriteti kompetent.

IS.I.OR.235 Kontraktimi i veprimtarive të menaxhimit të sigurisë së informacionit

a) Organizata siguron që gjatë kontraktimit të ndonjë pjese të aktiviteteve të përmendura në pikën IS.I.OR.200 me organizata të tjera, aktivitetet e kontraktuara janë në përputhje me kërkesat e kësaj Rregulloreje dhe organizata e kontraktuar punon nën mbikëqyrjen e saj. Organizata siguron që rreziqet që lidhen me aktivitetet e kontraktuara të menaxhohen siç duhet.

b) Organizata duhet të sigurojë që autoriteti kompetent të ketë akses nëpërmjet një kërkese ndaj organizatës së kontraktuar për të përcaktuar pajtueshmërinë e vazhdueshme me kërkesat e zbatueshme të përcaktuara në këtë Rregullore.

IS.I.OR.240 Kërkesat e personelit

a) Menaxheri përgjegjës i organizatës i caktuar në përputhje me urdhrin e ministrit nr. 79, datë 15.4.2024, "Për miratimin e rregullores mbi vazhdueshmërinë e vlefshmërisë ajrore të avionit dhe produkteve, pjesëve dhe pajisjeve aeronautike dhe mbi miratimin e organizatave dhe personelit të përfshirë në këto detyra", urdhrin e ministrit nr. 80, datë 30.6.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative për operimet ajrore", i ndryshuar; urdhrin e ministrit nr. 178, datë 20.12.2023, "Për miratimin e rregullores për kërkesat teknike dhe procedurat administrative në lidhje me ekuipazhin ajror të aviacionit civil", i ndryshuar; urdhrin e ministrit nr. 171, datë 11.11.2025, "Për miratimin e rregullores mbi përcaktimin e kërkesave teknike edhe procedurave administrative në lidhje me licencat dhe certifikatat e kontrollorëve të trafikut ajror"; urdhrin e ministrit nr. 193, datë 6.10.2022, "Për miratimin e rregullores për përcaktimin e kërkesave të përbashkëta për ofruesit e shërbimeve të menaxhimit të trafikut ajror dhe të lundrimit ajror, si dhe funksionet e tjera të rrjetit të menaxhimit të trafikut ajror dhe mbikëqyrjen e tyre", i ndryshuar; ose urdhrin e ministrit nr. 119, datë 29.9.2023, "Për miratimin e rregullores mbi kuadrin rregullator për hapësirën – U të hapësirës ajrore", siç është e zbatueshme e përmendur në nenin 2, pika 1 të kësaj Rregulloreje do të ketë autoritetin e korporatës për të siguruar që të gjitha aktivitetet e kërkuara nga kjo Rregullore të mund të financohen dhe kryhen. Ai person:

1. siguron që të gjitha burimet e nevojshme janë në dispozicion për të përmbushur kërkesat e kësaj Rregulloreje;

2. krijon dhe promovon politikën e sigurisë së informacionit të përmendur në pikën IS.I.OR.200(a)(1);

3. demonstron një njohuri bazë të kësaj Rregulloreje.

b) Menaxheri përgjegjës cakton një person ose grup personash për t'u siguruar që organizata është në përputhje me kërkesat e kësaj Rregulloreje dhe përcakton shtrirjen e autoritetit të tyre. Ai person ose grup personash i raporton drejtpërdrejt menaxherit përgjegjës dhe do të ketë njohuritë, përgatitjen dhe përvojën e duhur për të përmbushur përgjegjësitë e tyre. Në procedurë përcaktohet se kush e zëvendëson një person të caktuar në rast të mungesës së gjatë të atij personi.

c) Menaxheri përgjegjës emëron një person ose grup personash me përgjegjësinë për të menaxhuar funksionin e monitorimit të pajtueshmërisë të përmendur në pikën IS.I.OR.200(a)(12).

d) Kur organizata ndan strukturat organizative të sigurisë së informacionit, politikat, proceset dhe procedurat me organizata të tjera ose me pjesë të organizatës së tyre që nuk janë pjesë e miratimit, ose deklaratës, menaxheri përgjegjës mund t'ia delegojë aktivitetet e tij një personi përgjegjës të përbashkët.

Në një rast të tillë, krijohen masa koordinuese ndërmjet menaxherit përgjegjës të organizatës dhe personit të përbashkët përgjegjës për të siguruar integrimin e duhur të menaxhimit të sigurisë së informacionit brenda organizatës.

e) Menaxheri përgjegjës ose personi përgjegjës i përbashkët i përmendur në shkronjën "d" do të ketë autoritetin e korporatës për të krijuar dhe mirëmbajtur strukturat organizative, politikat, proceset dhe procedurat e nevojshme për zbatimin e pikës IS.I.OR.200.

f) Organizata duhet të ketë një proces për të siguruar që ka staf të mjaftueshëm në detyrë për të kryer aktivitetet e mbuluara nga ky aneks.

g) Organizata duhet të ketë një proces për të siguruar që stafi i përmendur në shkronjën "f" të ketë kompetencën e nevojshme për të kryer detyrat e tyre.

h) Organizata duhet të ketë një proces për të siguruar që stafi të pranojë dhe kuptojë përgjegjësitë që lidhen me rolet dhe detyrat e caktuara.

i) Organizata duhet të sigurohet që identiteti dhe besueshmëria e personelit të cilët kanë akses në sistemet e informacionit dhe të dhënat që u nënshtrohen kërkesave të kësaj Rregulloreje janë përcaktuar siç duhet.

IS.I.OR.245 Ruajtja e të dhënave

a) *Organizata duhet të ruajë të dhënat për aktivitetet e saj të menaxhimit të sigurisë së informacionit*

1. organizata duhet të sigurohet që të dhënat e mëposhtme të jenë të arkivuara dhe të gjurmueshme:

i. çdo miratim i marrë dhe çdo vlerësim shoqërues i rrezikut të sigurisë së informacionit në përputhje me pikën IS.I.OR.200(e);

ii. kontratat për aktivitetet e përmendura në pikën IS.I.OR.200(a)(9);

iii. të dhënat e proceseve kryesore të përmendura në pikën IS.I.OR.200(d);

iv. të dhënat e rreziqeve të identifikuara në vlerësimin e rrezikut të përmendur në pikën IS.I.OR.205, së bashku me masat shoqëruese të trajtimit të rrezikut të përmendura në pikën IS.I.OR.210;

v. të dhënat e incidenteve dhe cenueshmërive të sigurisë së informacionit të raportuara në përputhje me skemat e raportimit të përmendura në pikat IS.I.OR.215 dhe IS.I.OR.230;

vi. të dhënat e atyre ngjarjeve të sigurisë së informacionit që mund të kenë nevojë të rivlerësohen për të zbuluar incidente ose cenueshmëri të pazbuluara të sigurisë së informacionit.

2. të dhënat e përmendura në pikën (1)(i) ruhen të paktën deri në 5 vjet pasi miratimi të ketë humbur vlefshmërinë e tij;

3. të dhënat e përmendura në pikën (1)(ii) ruhen të paktën deri në 5 vjet pas ndryshimit ose përfundimit të kontratës;

4. të dhënat e përmendura në pikën (1)(iii), (iv) dhe (v) ruhen të paktën për një periudhë prej 5 vjetësh;

5. të dhënat e përmendura në pikën (1)(vi) mbahen derisa ato ngjarje të sigurisë së informacionit të rivlerësohen në përputhje me një periodicitet të përcaktuar në një procedurë të vendosur nga organizata;

b) *Organizata duhet të ruajë të dhëna për kualifikimin dhe trajnimin e stafit të vet të përfshirë në aktivitetet e menaxhimit të informacionit*

1. të dhënat e kualifikimit dhe përvojës së personelit ruhen për aq kohë sa personi punon për organizatën dhe për të paktën 3 vjet pasi personi të jetë larguar nga organizata.

2. anëtarëve të stafit, me kërkesën e tyre, u jepet akses në të dhënat e tyre individuale. Gjithashtu, me kërkesën e tyre, organizata do t'u sigurojë atyre një kopje të të dhënave të tyre individuale pas largimit nga organizata.

c) Formati i të dhënave duhet të specifikohet në procedurat e organizatës.

d) Të dhënat ruhen në një mënyrë që siguron mbrojtje nga dëmtimi, ndryshimi dhe vjedhja, me informacionin që identifikohet, kur kërkohet, sipas nivelit të klasifikimit të sigurisë. Organizata siguron që të dhënat të ruhen duke përdorur mjete për të siguruar integritetin, autenticitetin dhe aksesin e autorizuar.

IS.I.OR.250 Manuali i menaxhimit të sigurisë së informacionit (ISMM)

a) Organizata duhet t'i vërë në dispozicion autoritetit kompetent një manual për menaxhimin e sigurisë së informacionit (ISMM) dhe, sipas rastit, çdo manual përkatës dhe procedurë të përmendur, që përmban:

1. një deklaratë e nënshkruar nga menaxheri përgjegjës që konfirmon se organizata do të punojë në çdo kohë në përputhje me këtë aneks dhe me ISMM; nëse menaxheri i përgjegjshëm nuk është drejtori ekzekutiv (CEO) i organizatës, atëherë CEO duhet të bashkëfirmosë deklaratën;

2. titullin/jt, emrin/at, detyrat, llogaridhënien, përgjegjësitë dhe autorizimet e personit ose personave të përcaktuar në pikën IS.I.OR.240(b) dhe (c);

3. titullin, emrin, detyrat, llogaridhënien, përgjegjësitë dhe autoritetin e personit përgjegjës të përbashkët të përcaktuar në pikën IS.I.OR.240(d), sipas rastit;

4. politikën e sigurisë së informacionit të organizatës siç referohet në pikën IS.I.OR.200(a)(1);

5. një përshkrim të përgjithshëm të numrit dhe kategorive të personelit dhe të sistemit të vendosur për të planifikuar disponueshmërinë e personelit siç kërkohet nga pika IS.I.OR.240;

6. titujt, emrat, detyrat, llogaridhënien, përgjegjësitë dhe autoritetet e personave kryesorë përgjegjës për zbatimin e pikës IS.I.OR.200, duke përfshirë personin ose personat përgjegjës për funksionin e monitorimit të përputhshmërisë të përmendur në pika IS.I.OR.200(a)(12);

7. një organigramë që tregon zinxhirët përkatës të llogaridhënies dhe përgjegjësisë për personat e përmendur në pikat 2 dhe 6;

8. përshkrimin e skemës së raportimit të brendshëm të referuar në pikën IS.I.OR.215;

9. procedurat që përcaktojnë se si organizata siguron përputhjen me këtë pjesë, dhe në veçanti:

i. dokumentacionin e përmendur në pikën IS.I.OR.200(c);

ii. procedurat që përcaktojnë se si organizata kontrollon çdo aktivitet të kontraktuar, siç përmendet në pikën IS.I.OR.200(a)(9);

iii. procedurën e ndryshimit të ISMM-së të përmendur në shkronjën "c".

10. detajet e mjeteve alternative të pajtueshmërisë të miratuara aktualisht.

b) Botimi fillestar i ISMM-së do të miratohet dhe një kopje do të mbahet nga autoriteti kompetent. Për organizatat e deklaruara nuk do të kërkohet miratim. ISMM do të ndryshohet sipas nevojës për të mbetur një përshkrim i përditësuar i ISMMS-së së organizatës; një kopje e çdo ndryshimi në ISMM duhet t'i jepet autoritetit kompetent.

c) Ndryshimet në ISMM do të menaxhohen sipas procedurës së përcaktuar nga organizata. Çdo ndryshim që nuk përfshihet në objektin e kësaj procedure dhe çdo ndryshim në lidhje me ndryshimet e përmendura në pikën IS.I.OR.255(b) do të miratohet nga autoriteti kompetent. Për organizatat e deklaruara nuk do të kërkohet miratim.

d) Organizata mund të integrojë ISMM-në me prezantime ose manuale të tjera menaxheriale që disponon, me kusht që të ketë një referencë të qartë të kryqëzuar që tregon se cilat pjesë të prezantimit, ose manualit të menaxhimit përputhen me kërkesat e ndryshme të përfshira në këtë Aneks.

IS.I.OR.255 Ndryshime në sistemin e menaxhimit të sigurisë së informacionit

a) Ndryshimet në ISMS mund të kryhen dhe t'i njoftohen autoritetit kompetent në një procedurë të zhvilluar nga organizata. Kjo procedurë miratohet nga autoriteti kompetent, duke përjashtuar organizatat e deklaruara.

b) Në lidhje me ndryshimet në ISMS që nuk mbulohen nga procedura e përmendur në shkronjën "a", organizata duhet të aplikojë dhe të marrë një miratim të lëshuar nga autoriteti kompetent, duke përjashtuar organizatat e deklaruara, për të cilat nuk kërkohet miratim.

Në lidhje me këto ndryshime:

1. aplikimi duhet të dorëzohet përpara se të ndodhë një ndryshim i tillë, në mënyrë që t'i mundësojë autoritetit kompetent të përcaktojë pajtueshmërinë e vazhdueshme me këtë Rregullore dhe të ndryshojë, nëse është e nevojshme, certifikatën e organizatës dhe kushtet përkatëse të miratimit që i bashkëlidhen;

2. organizata do të vërë në dispozicion të autoritetit kompetent çdo informacion që kërkon për të vlerësuar ndryshimin;

3. ndryshimi do të zbatohet vetëm pas marrjes së një miratimi zyrtar nga autoriteti kompetent, duke përjashtuar organizatat e deklaruara, të cilat mund ta zbatojnë ndryshimin menjëherë;

4. organizata do të operojë sipas kushteve të përcaktuara nga autoriteti kompetent gjatë zbatimit të këtyre ndryshimeve.

IS.I.OR.260 Përmirësimi i vazhdueshëm

a) Organizata vlerëson, duke përdorur tregues të përshtatshëm të performancës, efektivitetin dhe pjekurinë e ISMS-së së saj. Vlerësimi kryhet mbi një bazë kalendarike të përcaktuar nga autoriteti kompetent ose pas një incidenti të sigurisë së informacionit.

b) Nëse konstatohen mangësi pas vlerësimit të kryer në përputhje me shkronjën "a", organizata merr masat e nevojshme të përmirësimit për të siguruar që ISMS-ja të vazhdojë të jetë në përputhje me kërkesat në fuqi dhe të mbajë rreziqet e sigurisë së informacionit në një nivel të pranueshëm. Përveç kësaj, organizata do të rivlerësojë ato elemente të ISMS-së të prekura nga masat e miratuara.