Svet
Evropske unije

Bruselj, 18. julij 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	14. julij 2022
Prejemnik:	Generalni sekretariat Sveta
Št. dok. Kom.:	C(2022) 4882 final - ANNEX
Zadeva:	PRILOGA k DELEGIRANI UREDBI KOMISIJE **o določitvi pravil za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu, za organizacije, zajete v uredbah Komisije (EU) št. 748/2012 in št. 139/2014, ter o spremembi uredb Komisije (EU) št. 748/2012 in št. 139/2014**

Delegacije prejmejo priloženi dokument C(2022) 4882 final - ANNEX.

Priloga: C(2022) 4882 final - ANNEX

EVROPSKA
KOMISIJA

Bruselj, 14.7.2022
C(2022) 4882 final

ANNEX

PRILOGA

k

DELEGIRANI UREDBI KOMISIJE

o določitvi pravil za uporabo Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta glede zahtev za obvladovanje tveganj za informacijsko varnost, ki lahko vplivajo na varnost v letalstvu, za organizacije, zajete v uredbah Komisije (EU) št. 748/2012 in št. 139/2014, ter o spremembi uredb Komisije (EU) št. 748/2012 in št. 139/2014

PRILOGA

INFORMACIJSKA VARNOST — ZAHTEVE ZA ORGANIZACIJE

[PART-IS.D.OR]

IS.D.OR.100 Področje uporabe

Ta del določa zahteve, ki jih morajo izpolnjevati organizacije iz člena 2 te uredbe.

IS.D.OR.200 Sistem upravljanja informacijske varnosti (ISMS)

(a) Za doseganje ciljev iz člena 1 organizacija vzpostavi, izvaja in vzdržuje sistem upravljanja informacijske varnosti (ISMS), ki zagotavlja, da organizacija:

1. oblikuje politiko o informacijski varnosti, ki določa splošna načela organizacije v zvezi z morebitnim učinkom tveganj za informacijsko varnost na varnost v letalstvu;

2. opredeli in pregleda tveganja za informacijsko varnost v skladu s točko IS.D.OR.205;

3. opredeljuje in izvaja ukrepe za obravnavo tveganj za informacijsko varnost v

skladu s točko IS.D.OR.210;

4. izvaja sistem notranjega poročanja o informacijski varnosti v skladu s točko IS.D.OR.215;

5. v skladu s točko IS.D.OR.220 opredeli in izvaja ukrepe, potrebne za zaznavanje dogodkov na področju informacijske varnosti, opredeli tiste dogodke, ki se štejejo za incidente, ki bi lahko vplivali na varnost v letalstvu, razen v primerih, ki jih dovoljuje točka IS.D.OR.205(e), ter se odziva na te informacijskovarnostne incidente in jih sanira;

6. izvaja ukrepe, ki jih je pristojni organ sporočil kot takojšen odziv na incident ali ranljivost v zvezi z informacijsko varnostjo, ki vpliva na varnost v letalstvu;

7. sprejme ustrezne ukrepe v skladu s točko IS.D.OR.225 za obravnavanje ugotovitev, ki jih je sporočil pristojni organ;

8. izvaja shemo zunanjega poročanja v skladu s točko IS.D.OR.230, da se pristojnemu organu omogoči sprejetje ustreznih ukrepov;

9. izpolnjuje zahteve iz točke IS.D.OR.235, kadar se kateri koli del dejavnosti iz točke IS.D.OR.200 odda v izvajanje drugim organizacijam;

10. izpolnjuje zahteve glede osebja iz točke IS.D.OR.240;

11. izpolnjuje zahteve glede vodenja evidenc iz točke IS.D.OR.245;

12. spremlja skladnost organizacije z zahtevami iz te uredbe in odgovornemu vodji ali, vodji projektivne organizacije v primeru projektivnih organizacij, zagotavlja povratne informacije o ugotovitvah, da se zagotovi učinkovito izvajanje korektivnih ukrepov;

13. brez poseganja v veljavne zahteve glede poročanja o incidentih varuje zaupnost vseh informacij glede na njihovo stopnjo občutljivosti, ki jih je organizacija morda prejela od drugih organizacij.

(b) Za stalno izpolnjevanje zahtev iz člena 1 organizacija izvaja postopek stalnega izboljševanja v skladu s točko IS.D.OR.260.

(c) Organizacija v skladu s točko IS.D.OR.250 dokumentira vse ključne procese, postopke, vloge in obveznosti, potrebne za skladnost s točko IS.D.OR.200(a), in vzpostavi proces za spremembo navedene dokumentacije. Spremembe navedenih procesov, postopkov, vlog in odgovornosti se upravljajo v skladu s točko IS.D.OR.255.

(d) Procesi, postopki, vloge in obveznosti, ki jih organizacija določi za skladnost s točko IS.D.OR.200(a), ustrezajo naravi in kompleksnosti njenih dejavnosti na podlagi ocene tveganj za informacijsko varnost, povezanih s temi dejavnostmi, in so lahko vključeni v druge obstoječe sisteme upravljanja, ki jih organizacija že izvaja.

(e) Brez poseganja v obveznost izpolnjevanja zahtev glede poročanja iz Uredbe (EU)

št. 376/2014([1]) in v zahteve iz točke IS.D.OR.200(a)(13) lahko pristojni organ organizaciji odobri, da ne izvaja zahtev iz točk (a) do (d) in povezanih zahtev iz točk IS.D.OR.205 do IS.D.OR.260, če navedenemu organu zadovoljivo dokaže, da njene dejavnosti, objekti in viri ter storitve, ki jih izvaja, prejema in vzdržuje, niti zase niti za druge organizacije ne predstavljajo nobenega tveganja za informacijsko varnost, ki bi lahko vplivalo na varnost v letalstvu. Odobritev temelji na dokumentirani oceni tveganja za informacijsko varnost, ki jo izvede organizacija ali tretja oseba v skladu s točko IS.D.OR.205 ter pregleda in odobri njen pristojni organ.

Nadaljnjo veljavnost navedene odobritve bo pregledal pristojni organ po veljavnem ciklu presoje nadzora in kadar se bodo izvedle spremembe na področju dela organizacije.

IS.D.OR.205 Ocena tveganja za informacijsko varnost

(a) Organizacija opredeli vse svoje elemente, ki bi lahko bili izpostavljeni tveganjem za informacijsko varnost. To vključuje:

1. dejavnosti, objekte in vire organizacije ter storitve, ki jih organizacija izvaja, zagotavlja, prejema ali vzdržuje;

2. opremo, sisteme, podatke in informacije, ki prispevajo k delovanju elementov iz točke (1).

(b) Organizacija opredeli vmesnike, ki jih ima z drugimi organizacijami in ki bi lahko povzročili vzajemno izpostavljenost tveganjem za informacijsko varnost.

(c) V zvezi z elementi in vmesniki iz točk (a) in (b) organizacija opredeli tveganja za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu. Organizacija za vsako ugotovljeno tveganje:

1. določi stopnjo tveganja v skladu z vnaprej določeno klasifikacijo organizacije;

2. poveže vsako tveganje in njegovo raven z ustreznim elementom ali vmesnikom, opredeljenim v skladu s točkama (a) in (b).

Pri vnaprej določeni klasifikaciji iz točke 1 se upoštevata možnost pojava scenarija grožnje in resnost njegovih posledic za varnost. Na podlagi navedene klasifikacije in ob upoštevanju, ali ima organizacija strukturiran in ponovljiv postopek upravljanja tveganja za operacije, je organizacija sposobna ugotoviti, ali je tveganje sprejemljivo ali ga je treba obravnavati v skladu s točko IS.D.OR.210.

Za lažjo medsebojno primerljivost ocen tveganj se pri določanju stopnje tveganja v skladu s točko 1 upoštevajo ustrezne informacije, pridobljene v sodelovanju z organizacijami iz točke (b).

([1]) Uredba (EU) št. 376/2014 Evropskega parlamenta in Sveta z dne 3. aprila 2014 o poročanju, analizi in spremljanju dogodkov v civilnem letalstvu, spremembi Uredbe (EU) št. 996/2010 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2003/42/ES Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 1321/2007 in (ES) št. 1330/2007 (UL L 122, 24.4.2014, str. 18).

(d) Organizacija pregleda in posodablja oceno tveganja, opravljeno v skladu s točkami (a), (b) in (c), v katerem koli od naslednjih primerov:

1. spremenijo se elementi, ki so izpostavljeni tveganjem za informacijsko varnost;

2. spremenijo se vmesniki med organizacijo in drugimi organizacijami ali tveganja, ki jih sporočijo druge organizacije;

3. spremenijo se informacije ali znanje, ki se uporabljajo za opredelitev, analizo in klasifikacijo tveganj;

4. pridobijo se izkušnje na podlagi analize informacijskovarnostnih incidentov.

IS.D.OR.210 Obravnava tveganja za informacijsko varnost

(a) Organizacija pripravi ukrepe za obravnavanje nesprejemljivih tveganj, ugotovljenih v skladu s točko IS.D.OR.205, jih pravočasno izvede in preveri njihovo nadaljnjo učinkovitost. Navedeni ukrepi organizaciji omogočajo:

1. nadzor nad okoliščinami, ki prispevajo k učinkovitemu nastanku scenarija grožnje;

2. zmanjšanje posledic za varnost v letalstvu, povezanih z uresničitvijo scenarija grožnje;

3. izogibanje tveganjem.

Navedeni ukrepi ne uvajajo novih morebitnih nesprejemljivih tveganj za varnost v letalstvu.

(b) Oseba iz točke IS.D.OR.240(a) in (b) ter drugo zadevno osebje organizacije se obvestijo o rezultatu ocene tveganja, izvedene v skladu s točko IS.D.OR.205, ustreznih scenarijih grožnje in ukrepih, ki jih je treba izvesti.

Organizacija obvesti tudi organizacije, s katerimi ima vmesnik v skladu s točko IS.D.OR.205(b), o kakršnem koli tveganju, ki je skupno obema organizacijama.

IS.D.OR.215 Sistem notranjega poročanja o informacijski varnosti

(a) Organizacija vzpostavi notranji sistem poročanja, da se omogoči zbiranje in ocenjevanje dogodkov v zvezi z informacijsko varnostjo, vključno s tistimi, o katerih je treba poročati v skladu s točko IS.D.OR.230.

(b) Navedena shema in postopek iz točke IS.D.OR.220 organizaciji omogočata, da:

1. ugotovi, kateri dogodki, sporočeni v skladu s točko (a), se štejejo za informacijskovarnostne incidente ali ranljivosti, ki bi lahko vplivali na varnost v letalstvu;

2. ugotovi vzroke in dejavnike, ki prispevajo k informacijskovarnostnim incidentom in ranljivostim, opredeljenim v skladu s točko (1), ter jih obravnava v okviru postopka upravljanja tveganja za informacijsko varnost v skladu s točkama IS.D.OR.205 in IS.D.OR.220;

3. zagotovi oceno vseh znanih, relevantnih informacij v zvezi z informacijskovarnostnimi incidenti in ranljivostmi, opredeljenimi v skladu s točko (1);

4. zagotovi izvajanje metode za interno razširjanje informacij po potrebi.

(c) Vsaka organizacija, ki je prevzela v izvajanje dejavnost, ki lahko organizacijo izpostavi tveganjem za informacijsko varnost, ki bi lahko vplivala na varnost v letalstvu, mora organizaciji poročati o dogodkih v zvezi z informacijsko varnostjo. Navedena poročila se predložijo po postopkih, določenih v posebnih pogodbenih dogovorih, in se ocenijo v skladu s točko (b).

(d) Organizacija pri preiskavah sodeluje s katero koli drugo organizacijo, ki znatno prispeva k informacijski varnosti lastnih dejavnosti.

(e) Organizacija lahko ta sistem poročanja vključi v druge sisteme poročanja, ki jih je že uvedla.

IS.D.OR.220 Informacijskovarnostni incidenti – zaznavanje, odzivanje in sanacija

(a) Organizacija na podlagi rezultata ocene tveganja, izvedene v skladu s točko IS.D.OR.205, in rezultata obravnave tveganja, izvedenega v skladu s točko IS.D.OR.210, izvaja ukrepe za zaznavanje incidentov in ranljivosti, ki kažejo na morebitno uresničitev nesprejemljivih tveganj in ki bi lahko vplivali na varnost v letalstvu. Ti ukrepi za zaznavanje omogočajo organizaciji, da:

1. opredeli odstopanja od vnaprej določenih izhodišč za funkcionalno učinkovitost;

2. sproži opozorila za aktiviranje ustreznih odzivnih ukrepov v primeru kakršnega koli odstopanja.

(b) Organizacija izvaja ukrepe za odziv na kakršne koli dogodke, opredeljene v skladu s točko (a), ki so prerasli v informacijskovarnostni incident ali bi vanj lahko prerasli. Ti ukrepi za odzivanje omogočajo organizaciji, da:

1. sproži odziv na opozorila iz točke (a)(2) z aktiviranjem vnaprej določenih virov in potekov ukrepov;

2. zajezi širjenje napada in prepreči, da bi se scenarij grožnje v celoti uresničil;

3. nadzira vrsto okvare prizadetih elementov, opredeljenih v točki IS.D.OR.205(a).

(c) Organizacija izvaja ukrepe za saniranje informacijskovarnostnih incidentov, po potrebi vključno z nujnimi ukrepi. Ti sanacijski ukrepi organizaciji omogočajo, da:

1. odpravi stanje, ki je povzročilo incident, ali ga omeji na sprejemljivo raven;

2. doseže varno stanje prizadetih elementov, opredeljenih v točki IS.D.OR.205(a), v času sanacije, ki ga je predhodno določila organizacija.

IS.D.OR.225 Odziv na ugotovitve, ki jih je sporočil pristojni organ

(a) Organizacija po prejemu obvestila o ugotovitvah, ki ga predloži pristojni organ:

1. opredeli temeljni vzrok ali vzroke za neskladnost in dejavnike, ki prispevajo k njej;

2. določi načrt korektivnih ukrepov;

3. pristojnemu organu zadovoljivo dokaže odpravo neskladnosti.

(b) Ukrepi iz točke (a) se izvedejo v roku, dogovorjenem s pristojnim organom.

IS.D.OR.230 Sistem zunanjega poročanja o informacijski varnosti

(a) Organizacija izvaja sistem poročanja o informacijski varnosti, ki izpolnjuje zahteve iz Uredbe (EU) št. 376/2014 ter njenih delegiranih in izvedbenih aktov, če se navedena uredba uporablja za organizacijo.

(b) Brez poseganja v obveznosti iz Uredbe (EU) št. 376/2014 organizacija zagotovi, da se o vsakem informacijskovarnostnem incidentu ali ranljivosti, ki lahko pomeni znatno tveganje za varnost v letalstvu, poroča njenemu pristojnemu organu. Poleg tega:

1. kadar tak incident ali ranljivost vpliva na zrakoplov ali z njim povezan sistem ali komponento, organizacija o tem poroča tudi nosilcu odobritve projekta;

2. kadar tak incident ali ranljivost vpliva na sistem ali komponento, ki jo uporablja organizacija, organizacija o tem poroča organizaciji, odgovorni za projektiranje sistema ali komponente.

(c) Organizacija poroča o pogojih iz točke (b), kot sledi:

1. obvestilo se predloži pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, takoj ko se organizacija seznani s stanjem;

2. poročilo se predloži pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, čim prej, vendar ne pozneje kot 72 ur od trenutka, ko se je organizacija seznanila s stanjem, razen če to preprečujejo izjemne okoliščine.

Poročilo se pripravi v obliki, ki jo določi pristojni organ, in vsebuje vse ustrezne informacije o stanju, s katerim je organizacija seznanjena;

3. pristojnemu organu in po potrebi nosilcu odobritve projekta ali organizaciji, odgovorni za projektiranje sistema ali komponente, se predloži nadaljnje poročilo, v katerem so podrobno navedeni ukrepi, ki jih je organizacija sprejela ali jih namerava sprejeti za sanacijo incidenta, in ukrepi, ki jih namerava sprejeti za preprečitev podobnih informacijskovarnostnih incidentov v prihodnosti.

   Nadaljnje poročilo se predloži takoj, ko so opredeljeni navedeni ukrepi, in se pripravi v obliki, ki jo določi pristojni organ.

IS.D.OR.235 Naročanje dejavnosti upravljanja informacijske varnosti

(a) Organizacija zagotovi, da pri oddaji naročila v zvezi s katerim koli delom dejavnosti iz točke IS.D.OR.200 drugim organizacijam, pogodbene dejavnosti izpolnjujejo zahteve iz te uredbe in da organizacija, ki je dejavnost prevzela v izvajanje, dela pod njenim nadzorom. Organizacija zagotovi, da se tveganja, povezana s pogodbenimi dejavnostmi, ustrezno obvladujejo.

(b) Organizacija zagotovi, da pristojni organ na zahtevo lahko dostopa do organizacije, ki je dejavnost prevzela v izvajanje, da preveri stalno skladnost z ustreznimi zahtevami iz te uredbe.

IS.D.OR.240 Zahteve za osebje

(a) Odgovorni vodja organizacije ali vodja projektivne organizacije v primeru projektivne organizacije, imenovan v skladu z uredbama (EU) št. 748/2012 in (EU) št. 139/2014, kot je navedeno v členu 2, točki 1(a) in (b), te uredbe, ima pooblastilo podjetja, da zagotovi financiranje in izvajanje vseh dejavnosti, ki jih zahteva ta uredba. Ta oseba:

   1. zagotovi, da so na voljo vsi potrebni viri za izpolnjevanje zahtev iz te uredbe;

   2. vzpostavi in spodbuja politiko informacijske varnosti iz točke IS.D.OR.200(a)(1);

   3. izkazuje osnovno razumevanje te uredbe.

(b) Odgovorni vodja ali vodja projektivne organizacije v primeru projektivne organizacije imenuje osebo ali skupino oseb za zagotovitev, da organizacija izpolnjuje zahteve iz te uredbe, in opredeli obseg svojih pooblastil. Navedena oseba ali skupina oseb poroča neposredno odgovornemu vodji ali vodji projektivne organizacije v primeru projektivne organizacije ter ima ustrezno znanje, izobrazbo in izkušnje za izvajanje svojih obveznosti. V postopkih se določi, kdo nadomešča določeno osebo v primeru njene daljše odsotnosti.

(c) Odgovorni vodja ali vodja projektivne organizacije v primeru projektivne organizacije imenuje osebo ali skupino oseb z obveznostjo za upravljanje funkcije spremljanja skladnosti iz točke IS.D.OR.200(a)(12).

(d) Kadar si organizacija deli organizacijske strukture, politike, procese in postopke za informacijsko varnost z drugimi organizacijami ali področji svoje organizacije, ki niso del odobritve ali izjave, lahko odgovorni vodja ali vodja projektivne organizacije v primeru projektivne organizacije prenese svoje dejavnosti na skupno odgovorno osebo.

V takem primeru se določijo usklajevalni ukrepi med odgovornim vodjo organizacije ali vodjo projektivne organizacije v primeru projektivnih organizacij in skupno odgovorno osebo, da se zagotovi ustrezna vključitev upravljanja informacijske varnosti v organizacijo.

(e) Odgovorni vodja ali vodja projektivne organizacije ali skupna odgovorna oseba iz točke (d) ima pooblastilo podjetja za vzpostavitev in vzdrževanje organizacijskih struktur, politik, procesov in postopkov, potrebnih za izvajanje točke IS.D.OR.200.

(f) Organizacija ima vzpostavljen postopek, s katerim zagotovi, da ima na delovnem mestu dovolj osebja za izvajanje dejavnosti iz te priloge.

(g) Organizacija ima vzpostavljen postopek za zagotovitev, da ima osebje iz točke (f) potrebno usposobljenost za opravljanje svojih nalog.

(h) Organizacija ima vzpostavljen postopek za zagotovitev, da osebje priznava odgovornosti, povezane z dodeljenimi vlogami in nalogami.

(i) Organizacija zagotovi, da sta identiteta in zaupanje v osebje, ki ima dostop do informacijskih sistemov in podatkov, za katere veljajo zahteve iz te uredbe, ustrezno določena.

IS.D.OR.245 Vodenje evidenc

(a) Organizacija vodi evidenco svojih dejavnosti upravljanja informacijske varnosti.

1. Organizacija zagotovi, da so naslednje evidence arhivirane in sledljive:

   (i) vse prejete odobritve in vse povezane ocene tveganja za informacijsko varnost v skladu s točko IS.D.OR.200(e);

   (ii) pogodbe za dejavnosti iz točke IS.D.OR.200(a)(9);

   (iii) evidence ključnih procesov iz točke IS.D.OR.200(d);

   (iv) evidence tveganj, opredeljenih v oceni tveganja iz točke IS.D.OR.205, skupaj s povezanimi ukrepi za obravnavo tveganja iz točke IS.D.OR.210;

   (v) evidence informacijskovarnostnih incidentov in ranljivosti, sporočenih v skladu s shemami poročanja iz točk IS.D.OR.215 in IS.D.OR.230;

   (vi) evidence dogodkov v zvezi z varnostjo informacij, ki jih bo morda treba ponovno oceniti, da se razkrijejo nezaznani informacijskovarnostni incidenti ali ranljivosti.

2. Evidence iz točke (1)(i) se hranijo najmanj pet let po prenehanju veljavnosti odobritve.

3. Evidence iz točke (1)(ii) se hranijo vsaj pet let po spremembi ali odpovedi pogodbe.

4. Evidence iz točk (1)(iii), (iv) in (v) se hranijo vsaj pet let.

5. Evidence iz točke (1)(vi) se hranijo, dokler se ti dogodki v zvezi z informacijsko varnostjo ponovno ne ocenijo v skladu s periodičnostjo, opredeljeno v postopku, ki ga določi organizacija.

(b) Organizacija vodi evidenco usposobljenosti in izkušenj svojega osebja, vključenega v dejavnosti upravljanja informacijske varnosti.

1. Evidence o usposobljenosti in izkušnjah osebja se hranijo toliko časa, dokler oseba dela za organizacijo, in vsaj tri leta po tem, ko oseba zapusti organizacijo.

2. Članom osebja se na njihovo zahtevo omogoči dostop do njihovih individualnih evidenc. Poleg tega jim organizacija na njihovo zahtevo zagotovi kopijo njihovih individualnih evidenc ob odhodu iz organizacije.

(c) Oblika evidenc se opredeli v postopkih organizacije.

(d) Evidence se hranijo na način, ki zagotavlja zaščito pred škodo, spremembo in tatvino, pri čemer se informacije, kadar je potrebno, opredelijo v skladu s stopnjo klasifikacije varnosti. Organizacija zagotovi, da se evidence hranijo s sredstvi za zagotovitev celovitosti, pristnosti in pooblaščenega dostopa.

IS.D.OR.250 Priročnik za upravljanje informacijske varnosti (ISMM)

(a) Organizacija da pristojnemu organu na voljo priročnik za upravljanje varnosti informacij (ISMM) in, kadar je ustrezno, vse pripadajoče priročnike in postopke, na katere se sklicuje, ki vsebuje:

1. izjavo, ki jo podpiše odgovorni vodja ali vodja projektivne organizacije v primeru projektivne organizacije, ki potrjuje, da bo organizacija ves čas delala v skladu s to prilogo in ISMM. Če odgovorni vodja ali v primeru projektivne organizacije vodja projektivne organizacije ni izvršni direktor organizacije, potem ta sopodpiše izjavo;

2. nazive, imena, dolžnosti, odgovornosti, obveznosti in pooblastila osebe ali oseb iz točke IS.D.OR.240(b) in (c);

3. naziv, ime, dolžnosti, odgovornosti, obveznosti in pooblastila skupne odgovorne osebe iz točke IS.D.OR.240(d), če je ustrezno;

4. politiko informacijske varnosti organizacije iz točke IS.D.OR.200(a)(1);

5. splošen opis števila in kategorij osebja ter sistema, vzpostavljenega za načrtovanje razpoložljivosti osebja, kot se zahteva v točki IS.D.OR.240(d);

6. nazive, imena, dolžnosti, odgovornosti, obveznosti in pooblastila ključnih oseb, odgovornih za izvajanje točke IS.D.OR.200, vključno z osebo ali osebami, odgovornimi za funkcijo spremljanja skladnosti iz točke IS.D.OR.200(a)(12);

7. organigram, ki prikazuje povezane verige odgovornosti in obveznosti za osebe iz točk (2) in (6);

8. opis sistema notranjega poročanja iz točke IS.D.OR.215;

9. postopke, ki določajo, kako organizacija zagotavlja skladnost s tem delom, in zlasti:

(i) dokumentacijsko točko IS.D.OR.200(c);

(ii) postopke, ki opredeljujejo, kako organizacija nadzira katere koli pogodbene dejavnosti iz točke IS.D.OR.200(a)(9);

(iii) postopek spremembe ISMM, opredeljen v točki (c);

10. podrobnosti trenutno odobrenih drugih načinov usklajevanja.

(b) Prva izdaja ISMM se odobri, kopijo pa obdrži pristojni organ. ISMM se po potrebi spremeni, da ostaja ažuren opis sistema ISMS organizacije. Pristojnemu organu se predloži kopija vseh sprememb ISMM.

(c) Spremembe ISMM se upravljajo po postopku, ki ga določi organizacija. Pristojni organ odobri vse spremembe, ki niso vključene v področje uporabe tega postopka, in vse spremembe, povezane s spremembami, navedenimi v točki IS.D.OR.255(b).

(d) Organizacija lahko ISMM poveže z drugimi priročniki za upravljanje ali priročniki, ki jih hrani, če obstaja jasna navzkrižna referenca, ki navaja, kateri deli priročnika za upravljanje ustrezajo različnim zahtevam iz te priloge.

IS.D.OR.255 Spremembe sistema upravljanja informacijske varnosti

(a) Spremembe sistema ISMS se lahko upravljajo in sporočijo pristojnemu organu s postopkom, ki ga razvije organizacija. Ta postopek odobri pristojni organ.

(b) V zvezi s spremembami sistema ISMS, ki niso zajete v postopku iz točke (a), organizacija zaprosi za odobritev pristojnega organa in jo pridobi.

V zvezi s temi spremembami:

1. se zahtevek predloži pred izvedbo vsake takšne spremembe, da bi pristojni organ lahko ugotovil, ali je zagotovljena stalna skladnost s to uredbo, in da bi po potrebi spremenil certifikat organizacije in z njim povezane pogoje za odobritev, ki so mu priloženi;

2. organizacija da pristojnemu organu na voljo vse informacije, ki jih zahteva za oceno spremembe;

3. se sprememba izvede šele po prejemu uradne odobritve pristojnega organa;

4. organizacija med izvajanjem takih sprememb deluje pod pogoji, ki jih predpiše pristojni organ.

IS.D.OR.260 Stalno izboljševanje

(a) Organizacija z ustreznimi kazalniki uspešnosti oceni učinkovitost in zrelost sistema ISMS. Ta ocena se izvede na podlagi koledarja, ki ga organizacija vnaprej določi, ali po informacijskovarnostnem incidentu.

(b) Če se po oceni, opravljeni v skladu s točko (a), ugotovijo pomanjkljivosti, organizacija sprejme potrebne ukrepe za izboljšanje, s katerimi zagotovi, da ISMS še naprej izpolnjuje veljavne zahteve in tveganja za informacijsko varnost ohranja na sprejemljivi ravni. Poleg tega organizacija ponovno oceni tiste elemente sistema ISMS, na katere so vplivali sprejeti ukrepi.