UE

GUVERNUL REPUBLICII MOLDOVA

H O T Ă R Â R E nr. ____

din 2025

Chișinău

cu privire la aprobarea Regulamentului privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației și modificarea unor hotărâri ale Guvernului

---

În temeiul art. 6 alin. (3) lit. a) din Codul aerian al Republicii Moldova nr. 301/2017 (Monitorul Oficial al Republicii Moldova, 2018, nr. 95-104, art.189), cu modificările ulterioare, Guvernul

HOTĂRĂŞTE:

1. Se aprobă:

1.1. Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, conform anexei nr.1;

1.2. Modificările ce se operează în unele hotărârâri ale Guvernului, conform anexei nr. 2.

2. Prevederile pct. 1 subpct. 1.1. și 1.2., ale pct. 2. subpct. 2.1., 2.2. și 2.3. din Anexa nr. 2 la prezenta hotărâre intră în vigoare la data de 16 octombrie 2025.

3. Prezenta hotărâre se publică în Monitorul Oficial al Republicii Moldova și intră în vigoare la data de 22 februarie 2026.

PRIM – MINISTRU **Dorin RECEAN**

Contrasemnează:
Viceprim-ministru, ministrul infrastructurii și dezvoltării regionale **Vladimir BOLEA**

Anexa nr. 1
la Hotărârea Guvernului nr.___/2025

REGULAMENTUL
privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației

Prezentul Regulament transpune total:

- **Regulamentul delegat (UE) 2022/1645** al Comisiei din 14 iulie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei și de modificare a Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei, **CELEX: 32022R1645**, publicat în Jurnalul Oficial al Uniunii Europene L 248/18 din 26 septembrie 2022.

- **Regulamentul de punere în aplicare (UE) 2023/203** al Comisiei din 27 octombrie 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, precum și autorităților competente care intră sub incidența Regulamentelor (UE) nr. 748/2012, (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340 și (UE) nr. 139/2014 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, și de modificare a Regulamentelor (UE) nr. 1178/2011, (UE) nr. 748/2012, (UE) nr. 965/2012, (UE) nr. 139/2014, (UE) nr. 1321/2014, (UE) 2015/340 ale Comisiei și a Regulamentelor de punere în aplicare (UE) 2017/373 și (UE) 2021/664 ale Comisiei, **CELEX: 32023R0203**, publicat în Jurnalul Oficial al Uniunii Europene L 31 din 02 februarie 2023, astfel cum a fost modificat ultima oară prin Regulamentul de punere în aplicare (UE) 2023/1769 al Comisiei din 12 septembrie 2023 de stabilire a cerințelor tehnice și a procedurilor administrative pentru aprobarea organizațiilor implicate în proiectarea sau producția de sisteme și componente de management al traficului aerian/servicii de navigație aeriană și de modificare a Regulamentului de punere în aplicare (UE) 2023/203.

CAPITOLUL I
OBIECTUL ȘI DOMENIU DE APLICARE

1. Prezentul Regulament stabilește cerințe pe care trebuie să le îndeplinească organizațiile și autoritățile naționale în vederea:

1.1. identificării și a managementului riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care ar putea afecta sistemele de tehnologie a informației și comunicațiilor și datele utilizate în scopul aviației civile;

1.2. detectării evenimentelor de securitate a informațiilor și a identificării celor care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației;

1.3. asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.

2. Prezentul Regulament se aplică următoarelor organizații:

2.1. organizațiilor de producție și organizațiilor de proiectare supuse dispozițiilor din secțiunea A Capitolul G și J din anexa nr. 1 PARTEA 21 la Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024, cu excepția organizațiilor de proiectare și producție care sunt implicate exclusiv în proiectarea și/sau producția de aeronave ELA2, astfel cum sunt definite la pct. 2 din Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024;

2.2. organizațiilor de întreținere supuse dispozițiilor din secțiunea A din Anexa nr. 2 (partea 145) la Regulamentul privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, cu excepția celor implicate exclusiv în întreținerea aeronavelor în conformitate cu anexa nr. 5b (partea ML);

2.3. organizațiilor de management al continuității navigabilității (CAMO-uri) supuse dispozițiilor din secțiunea A din Anexa nr. 5c (partea CAMO) la Regulamentul privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, cu excepția celor implicate exclusiv în managementul continuității navigabilității aeronavelor în conformitate cu anexa nr. 5b (partea ML);

2.4. operatorilor de aerodromuri și furnizorilor de servicii de gestionare a platformei care sunt supuși dispozițiilor din Anexa nr. 2 „CERINŢE APLICABILE ORGANIZAŢIILOR (ADR.OR)” la Regulamentul privind procedurile administrative referitoare la aerodromuri, aprobat prin Hotărârea de Guvern nr. 653/2018;

2.5. operatorilor aerieni supuși dispozițiilor din Anexa nr. 3 (partea ORO) la Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, aprobat prin Hotărârea de Guvern nr. 612/2022, cu excepția celor implicați exclusiv în operarea oricăreia dintre următoarele:

2.5.1. o aeronavă ELA 2, astfel cum este definită la pct. 2 din Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi

echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024;

2.5.2. avioane monomotoare cu elice cu o configurație maximă operațională de cinci locuri pentru pasageri sau mai puțin, care nu sunt clasificate drept aeronave complexe motorizate, atunci când decolează și aterizează pe același aerodrom sau loc de operare și când operează în conformitate cu regulile de zbor la vedere (VFR) pe timp de zi;

2.5.3. elicoptere monomotoare cu o configurație maximă operațională de cinci locuri pentru pasageri sau mai puțin, care nu sunt clasificate drept aeronave complexe motorizate, atunci când decolează și aterizează pe același aerodrom sau loc de operare și când operează în conformitate cu regulile de zbor la vedere (VFR) pe timp de zi;

2.6. organizațiilor de pregătire aprobate (ATO-uri) supuse dispozițiilor din Anexa nr. 7 (partea ORA) la Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, aprobat prin Hotărârea de Guvern nr. 204/2020, cu excepția celor implicate exclusiv în activități de pregătire aferente aeronavelor ELA 2, astfel cum este definită la pct. 2 din Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024, sau implicate exclusiv în pregătire teoretică;

2.7. centrelor de medicină aeronautică pentru personalul navigant supuse dispozițiilor din Anexa nr. 7 (partea ORA) la Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, aprobat prin Hotărârea de Guvern nr. 204/2020;

2.8. operatorilor de echipamente de pregătire sintetică pentru zbor (FSTD-uri) supuși dispozițiilor din Anexa nr. 7 (partea ORA) la Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, aprobat prin Hotărârea de Guvern nr. 204/2020, cu excepția celor implicați exclusiv în operarea FSTD-urilor aferente aeronavelor ELA 2, astfel cum este definită la pct. 2 din Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024;

2.9. organizațiilor de pregătire a controlorilor de trafic aerian (ATCO) și centrele de medicină aeronautică pentru ATCO supuse dispozițiilor din Anexa nr. 2 (partea ATCO.OR) la Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, aprobat prin Hotărârea de Guvern nr. 134/2019;

2.10. organizațiilor supuse dispozițiilor din Anexa nr. 3 (partea ATM/ANS.OR) la Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, aprobat prin Hotărârea de Guvern nr. 119/2023, cu excepția următorilor furnizori de servicii:

2.10.1. furnizorilor de servicii de navigație aeriană care dețin un certificat limitat în conformitate cu pct. ATM/ ANS.OR.A.010 din anexa menționată;

2.10.2. furnizorilor de servicii de informare a zborurilor care își declară activitățile în conformitate cu pct ATM/ ANS.OR.A.015 din anexa menționată;

2.11. furnizorilor de servicii U-space și furnizorilor unici de servicii de informații;

2.12. organizațiilor aprobate implicate în proiectarea sau producția de sisteme ATM/ANS și de componente ATM/ANS;

CAPITOLUL II
PREVEDERI GENERALE

3. În sensul prezentului Regulament se aplică următoarele noțiuni:

3.1. *amenințare* - o încălcare potențială a securității informațiilor care există atunci când o entitate, o circumstanță, o acțiune sau un eveniment ar putea cauza prejudicii;

3.2. *eveniment de securitate a informațiilor* - un eveniment identificat al unui sistem, al unui serviciu sau al unei rețele, care indică o posibilă încălcare a politicii de securitate a informațiilor sau o deficiență a controalelor de securitate a informațiilor, ori o situație necunoscută anterior care poate fi relevantă pentru securitatea informațiilor;

3.3. *incident* - orice eveniment care are un efect negativ asupra securității rețelelor și sistemelor informatice;

3.4. *risc în materie de securitate a informațiilor* - riscul la adresa organizării operațiunilor aeronautice, precum și la adresa activelor, persoanelor fizice și a altor organizații, atribuit unui posibil eveniment de securitate a informațiilor. Riscurile în materie de securitate a informațiilor sunt asociate cu posibilitatea ca amenințările să exploateze vulnerabilitățile unui activ informațional sau ale unui grup de active informaționale;

3.5. *securitatea informațiilor* - păstrarea confidențialității, integrității, autenticității și disponibilității rețelelor și sistemelor informatice;

3.6. *vulnerabilitate* - o deficiență sau slăbiciune a unui activ sau a unui sistem, a procedurilor, a concepției, a implementării sau a măsurilor de securitate a informațiilor, care ar putea fi exploatată și s-ar putea solda cu o încălcare sau nerespectare a politicii de securitate a informațiilor.

4. Autoritatea responsabilă de supravegherea şi controlul respectării prevederilor prezentului Regulament de către organizațiile menționate la pct. 2 este autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile - *Autoritatea Aeronautică Civilă (în continuare – „AAC”)*.

5. AAC, în vederea realizării supravegherii şi controlul respectării prevederilor prezentului Regulament, antrenează în activitatea sa autoritatea competentă la nivel naţional în domeniul securităţii cibernetice - *Agenția pentru Securitatea Cibernetică (în continuare „ASC”)*, în conformitate cu prevederile Regulamentului cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea de Guvern nr. 1028/2023 și altor acte conexe.

6. AAC, în conformitate cu prevederile pct. 6 subpct. 3) - 4) și prevederile pct. 7 subpct. 4) din Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, aprobat prin Hotărârea de Guvern nr. 1028/2023, comunică, fără întârzieri nejustificate, punctului unic de contact – ASC, orice informație relevantă inclusă în notificările transmise în temeiul pct. 8. IS.I.OR.230 și al pct. 22. IS.D.OR.230 din Anexa nr. 2 la prezentul Regulament, de către operatorii de servicii esențiale identificați.

7. În vederea realizării prevederilor pct. 5 și pct. 6, ASC și AAC vor stabili măsuri comune de coordonare pentru a se asigura supravegherea efectivă a tuturor cerințelor care trebuie respectate de către organizații.

8. Cerințele aplicabile organizațiilor prevăzute la pct. 2 sunt stabilite în Anexa nr. 2 [PARTEA IS.D.OR] și [PARTEA IS.I.OR], la prezentul Regulament.

9. Cerințele aplicabile AAC sunt stabilite în Anexa nr. 1 [PARTEA IS.AR], la prezentul Regulament.

10. Prevederile prezentului Regulament sunt aplicabile și în cazul în care o organizație menționată la pct. 2 este un operator sau o entitate care dispune de date, informații, rețele sau sisteme informaționale de importanța critică din punct de vedere a securității aeronautice în sensul Legii nr. 192/2019 privind securitatea aeronautică.

11. Implementarea și aplicarea prevederilor prezentului Regulament se realizează în deplină conformitate cu normele aplicabile privind confidențialitatea, protecția datelor cu caracter personal și protecția informațiilor clasificate potrivit legislației corespunzătoare.

Anexa nr. 1
La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației

SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE AAC [PARTEA IS.AR]

1. IS.AR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele în materie de management care trebuie îndeplinite de AAC când își desfășoară activitățile de certificare, de supraveghere și de asigurare a respectării conformității.

2. IS.AR.200 Sistemul de management al securității informațiilor (SMSI)

2.1. Pentru a atinge obiectivele prevăzute la pct. 1, AAC instituie, implementează și menține un sistem de management al securității informațiilor (SMSI) care asigură faptul că aceasta:

2.1.1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;

2.1.2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu pct. 3. IS.AR.205;

2.1.3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu pct. 4. IS.AR.210;

2.1.4. definește și implementează, în conformitate cu pct. 5. IS.AR.215, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, asigură un răspuns la respectivele incidente de securitate a informațiilor și le redresează în urma acestora;

2.1.5. îndeplinește cerințele de la pct. 6. IS.AR.220 când subcontractează altor organizații orice parte a activităților descrise la pct. 2. IS.AR.200;

2.1.6. îndeplinește cerințele în materie de personal de la pct. 7. IS.AR.225;

2.1.7. îndeplinește cerințele de păstrare a evidențelor de la pct. 8. IS.AR.230;

2.1.8. monitorizează îndeplinirea de către propria instituție a cerințelor din prezentul Regulament și transmite persoanei menționate la subpct.7.1. IS.AR.225 feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

2.1. 9. protejează confidențialitatea oricăror informații cu privire la organizații care fac obiectul supravegherii sale și a informațiilor primite prin intermediul sistemelor de raportare externă ale organizației, instituite în conformitate cu pct. 8. IS.I.OR.230 și cu pct. 22. IS.D.OR.230 din Anexa nr. 2 la prezentul Regulament;

2.1.10. notifică ASC schimbările care afectează capacitatea AAC de a-și executa sarcinile și de a-și îndeplini responsabilitățile definite în prezentul Regulament;

2.1.11. definește și pune în aplicare proceduri pentru transmiterea informațiilor pertinente, în funcție de necesități și într-un mod practic și rapid, pentru a ajuta organizațiile supuse dispozițiilor prezentului Regulament să efectueze evaluări eficace ale riscurilor în materie de securitate asociate activităților lor.

2.2. Pentru a îndeplini în permanență cerințele menționate la pct. 1, AAC trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu pct. 9. IS.AR.235.

2.3. AAC documentează toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma subpct. 2.1. IS.AR.200 și instituie un proces de modificare a acestei documentații.

2.4. Procesele, procedurile, rolurile și responsabilitățile instituite de AAC pentru a se conforma subpct. 2.1. IS.AR.200 trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de AAC.

3. IS.AR.205 Evaluarea riscurilor în materie de securitate a informațiilor

3.1. AAC trebuie să identifice toate elementele în actvitatea sa care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea cuprind:

3.1.1. activitățile, instalațiile și resursele, serviciile pe care le operează, furnizează, primește sau menține;

3.1.2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor menționate la subpct. 3.1.1.

3.2. AAC trebuie să identifice interfețele pe care propria instituție le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

3.3. Pentru elementele și interfețele menționate la subpct. 3.1. și la subpct. 3.2., AAC trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.

Pentru fiecare risc identificat, AAC trebuie:

3.3.1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită;

3.3.2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu subpct. 3.1. și pct. 3.2.

Clasificarea predefinită menționată la subpct. 3.1.1. trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Prin această clasificare și în funcție de existența sau absența, în cadrul AAC, a unui proces structurat și repetabil de management al riscurilor pentru operațiuni, AAC trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu pct. 4. IS.AR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în conformitate cu subpct. 3.1.1. se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la subpct. 3.2.

3.4. AAC trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu subpunct. 3.1., 3.2. și 3.3. în oricare dintre următoarele cazuri:

3.4.1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

3.4.2. când există o modificare a interfețelor dintre AAC și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

3.4.3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

3.4.4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

4. IS.AR.210 Tratarea riscurilor în materie de securitate a informațiilor

4.1. AAC trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu pct. 3. IS.AR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită AAC:

4.1.1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

4.1.2. să diminueze consecințele pentru siguranța aviației care sunt asociate materializării scenariului de amenințare;

4.1.3. să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

4.2. Persoana menționată la subpct. 7.1. IS.AR.225 și ceilalți membri vizați ai personalului AAC trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu pct. 3. IS.AR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate.

AAC trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu subpct. 3.2. IS.AR.205 cu privire la orice risc comun.

5. IS.AR.215 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

5.1. În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu pct.3. IS.AR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu pct. 4. IS.AR.210, AAC trebuie să implementeze măsuri de detectare a evenimentelor care indică materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită AAC:

5.1.1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

5.1.2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

5.2. AAC trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu subpunct. 5.1. care se pot transforma ori s-au transformat

într-un incident de securitate a informațiilor. Respectivele măsuri de răspuns trebuie să permită AAC:

5.2.1. să declanșeze reacția propriei instituții la avertizările menționate la subpct. 5.1.2. prin activarea unor resurse și planuri de acțiune predefinite;

5.2.2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

5.2.3. să controleze modul de defectare al elementelor afectate definite la subpct. 3.1. IS.AR.205.

5.3. AAC trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită AAC:

5.3.1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

5.3.2. să restabilească starea de siguranță a elementelor afectate definite la subpct. IS.AR.205 în timpul de redresare definit în prealabil de propria instituția.

6. IS.AR.220 Subcontractarea activităților de management al securității informațiilor

AAC trebuie să se asigure, atunci când subcontractează altor instituții orice parte a activităților menționate la pct. 6. IS.AR.200, că activitățile subcontractate respectă cerințele din prezentul Regulament și că instituția subcontractată lucrează sub supravegherea sa. AAC trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

7. IS.AR.225 Cerințele în materie de personal

AAC trebuie:

7.1. să dispună de o persoană care are drepturile statutare necesare pentru a institui și a menține structurile organizaționale, politicile, procesele și procedurile necesare pentru punerea în aplicare a prezentului regulament.

Această persoană trebuie:

7.1.1. să aibă drepturile statutare pentru accesarea deplină a resurselor necesare pentru ca AAC să îndeplinească toate sarcinile prevăzute în prezentul Regulament;

7.1.2. să dețină delegarea de competențe necesară pentru îndeplinirea atribuțiilor primite;

7.2. să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru desfășurarea activităților reglementate de prezenta Anexă;

7.3. să dispună de o procedură prin care să se asigure că personalul menționat la subpunct.7.2. are competența necesară pentru a-și îndeplini sarcinile;

7.4. să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite;

7.5. să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului Regulament sunt stabilite în mod corespunzător.

8. IS.AR.230 Păstrarea evidențelor

8.1. AAC trebuie să păstreze evidența activităților sale de management al securității informațiilor.

8.1.1. AAC asigură că următoarele evidențe sunt arhivate și trasabile:

8.1.1.1. contractele pentru activitățile menționate la subpct. 2.1.5. IS.AR.200;

8.1.1.2. evidențele proceselor-cheie menționate la subpct. 2.4. IS.AR.200;

8.1.1.3. evidențele riscurilor identificate în evaluarea riscurilor menționată la pct. 3 IS.AR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la pct. 4 IS.AR.210;

8.1.1.4. evidențele evenimentelor de securitate a informațiilor care ar putea necesita o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

8.1.2. Evidențele menționate la subpct. 8.1.1.1. se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

8.1.3. Evidențele menționate la subpct. 8.1.1.2. și 8.1.1.3. se păstrează timp de cel puțin cinci ani.

8.1.4. Evidențele menționate la subpct. 8.1.1.4. se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de AAC.

8.2. AAC trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.

8.2.1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru AAC și timp de cel puțin trei ani după ce persoana a părăsit AAC.

8.2.2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, AAC trebuie să le furnizeze acestora, la părăsirea AAC, o copie a evidențelor personale.

8.3. Formatul evidențelor se specifică în procedurile AAC.

8.4. Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. AAC trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

9. IS.AR.235 Îmbunătățirea continuă

9.1. AAC trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea propriului SMSI. Evaluarea trebuie efectuată pe baza unui calendar predefinit, stabilit de AAC, sau în urma unui incident de securitate a informațiilor.

9.2. Dacă în urma evaluării efectuate în conformitate cu subpct. 9.1. se constată deficiențe, AAC trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să respecte cerințele aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, AAC trebuie să reevalueze elementele SMSI-ului vizate de măsurile adoptate.

Anexa nr. 2
La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației

SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE ORGANIZAȚIILOR

[PARTEA IS.I.OR]

1. IS.I.OR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la pct. 2 din prezentul Regulament cu excepția subpct. 2.1. și subpct. 2.4.

2. IS.I.OR.200 Sistemul de management al securității informațiilor (SMSI)

2.1. Pentru a atinge obiectivele prevăzute la pct. 1 din Regulament, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația:

2.1.1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale organizației în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;

2.1.2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu pct. 3. IS.I.OR.205;

2.1.3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu pct. 4. IS.I.OR.210;

2.1.4. implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu pct. 5. IS.I.OR.215;

2.1.5. definește și implementează, în conformitate cu pct. 6. IS.I.OR.220, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, cu excepția cazurilor permise conform subpct. 3.5. IS.I.OR.205, asigură un răspuns la respectivele incidentele de securitate a informațiilor și se redresează în urma acestora;

2.1.6. implementează măsurile care au fost notificate de AAC ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației;

2.1.7. ia măsurile corespunzătoare, în conformitate cu pct. 7. IS.I.OR.225, pentru abordarea constatărilor notificate de AAC;

2.1.8. implementează un sistem de raportare externă în conformitate cu pct. 8. IS.I.OR.230, astfel încât AAC să poată lua măsuri corespunzătoare;

2.1.9. îndeplinește cerințele de la pct. 9. IS.I.OR.235 când subcontractează altor organizații orice parte a activităților menționate la pct. 2. IS.I.OR.200;

2.1.10. îndeplinește cerințele în materie de personal stabilite la pct. 10. IS.I.OR.240;

2.1.11. îndeplinește cerințele de păstrare a evidențelor stabilite la pct. 11. IS.I.OR.245;

2.1.12. monitorizează îndeplinirea de către organizație a cerințelor din prezentul Regulament și transmite managerului responsabil feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

2.1.13. protejează, fără a aduce atingere cerințelor aplicabile în materie de raportare a incidentelor, confidențialitatea oricăror informații pe care organizația le-ar fi putut primi de la alte organizații, în funcție de nivelul de sensibilitate a informațiilor respective.

2.2. Pentru a îndeplini în permanență cerințele menționate la subpct. 2.1.1., organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu pct. 14. IS.I.OR.260.

2.3. Organizația trebuie să documenteze, în conformitate cu pct. 12. IS.I.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma subpct. 2.1. IS.I.OR.200 și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu pct. 13. IS.I.OR.255.

2.4. Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma subpct. 2.1. IS.I.OR.200 trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de organizație.

2.5. Fără a se aduce atingere obligației de conformitate cu cerințele de raportare stabilite în reglementarea aeronautică civilă „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la evenimentele de aviaţie civilă”, aprobate prin Ordinul MIDR nr. 119/2020 și cu cerințele stabilite la subpct. 2.1.13. IS.I.OR.200, organizația poate primi din partea AAC aprobarea de a nu implementa cerințele menționate la subpct. 2.1. – subpct. 2.5. și cerințele aferente de la pct. 3. IS.I.OR.205 - pct. 14. IS.I.OR.260 dacă demonstrează într-un mod considerat satisfăcător de AAC că activitățile, instalațiile și resursele sale, precum și serviciile pe care le operează, furnizează, primește și menține nu prezintă niciun risc în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației pentru organizația în sine sau pentru alte organizații. Aprobarea trebuie să se bazeze pe o evaluare documentată a riscurilor în materie de securitate a informațiilor, efectuată de organizație sau de o parte terță în conformitate cu pct. 3. IS.I.OR.205 și examinată și aprobată de AAC.

Menținerea valabilității respectivei aprobări va fi examinată de AAC în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.

3. IS.I.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor

3.1. Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă:

3.1.1. activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația;

3.1.2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpct. 3.1.1.

3.2. Organizația trebuie să identifice interfețele pe care le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

3.3. În ceea ce privește elementele și interfețele menționate la subpct. 3.1. și subpct. 3.2., organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie:

3.3.1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație;

3.3.2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu subpct. 3.1. și subpct. 3.2.

Clasificarea predefinită menționată la subpct. 3.1.1. trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Pe baza acestei clasificări și în funcție de existența sau absența, în cadrul organizației, a unui proces structurat și repetabil de management al riscurilor pentru operațiuni, organizația trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu pct. 4. IS.I.OR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în temeiul subpct. 3.1.1. se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la subpct. 3.2.

3.4. Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu subpct. 3.1., subpct. 3.2. și, după caz, subpct. 3.3. sau subpct. 3.5. în oricare dintre următoarele situații:

3.4.1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

3.4.2. când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

3.4.3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

3.4.4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

3.5. Prin derogare de la subpct. 3.3., organizațiile care trebuie să respecte subpartea C din Anexa nr. 3 (partea ATM/ANS.OR) la Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, aprobat prin Hotărârea de Guvern nr. 119/2023, înlocuiesc analiza impactului asupra siguranței aviației cu o analiză a impactului asupra serviciilor lor, în conformitate cu evaluarea în sprijinul siguranței prevăzută la pct. ATM/ANS.OR.C.005. Această evaluare în sprijinul siguranței se pune la dispoziția furnizorilor de servicii de trafic aerian cărora organizațiile le furnizează servicii, iar respectivii furnizori de servicii de trafic aerian sunt responsabili cu evaluarea impactului asupra siguranței aviației.

4. IS.I.OR.210 Tratarea riscurilor în materie de securitate a informațiilor

4.1. Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu pct. 3. IS.I.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației:

4.1.1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

4.1.2. să diminueze consecințele asupra siguranței aviației care sunt asociate materializării scenariului de amenințare;

4.1.3. să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

4.2. Persoana menționată la subpct. 10.1. și subpct. 10.2. IS.I.OR.240 și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu pct. 3. IS.I.OR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate.

Organizația trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu subpct. 3.2. IS.I.OR.205 cu privire la orice risc comun celor două organizații.

5. IS.I.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor

5.1. Organizația trebuie să instituie un sistem de raportare internă pentru a permite colectarea și evaluarea evenimentelor legate de securitatea informațiilor, inclusiv a celor care trebuie raportate în temeiul pct. 8. IS.I.OR.230.

5.2. Sistemul respectiv și procesul menționat la pct. 6. IS.I.OR.220 trebuie să permită organizației:

5.2.1. să identifice care dintre evenimentele raportate în temeiul subpct. 5.1. sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației;

5.2.2. să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpct. 5.2.1 și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu pct. 3. IS.I.OR.205 și pct. 6. IS.I.OR.220;

5.2.3. să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpct. 5.2.1.;

5.2.4. să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.

5.3. Orice organizație subcontractată care ar putea expune organizația la riscuri în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației are obligația de a raporta organizației evenimentele de securitate a informațiilor. Rapoartele respective se transmit prin procedurile stabilite în angajamentele contractuale specifice și se evaluează în conformitate cu subpct. 5.2.

5.4. Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.

5.5. Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.

6. IS.I.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

6.1. În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu pct. 3. IS.I.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu pct. 4. IS.I.OR.210, organizația trebuie să implementeze măsuri de detectare a incidentelor și vulnerabilităților care să indice materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită organizației:

6.1.1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

6.1.2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

6.2. Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu subpct. 6.1. care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Respectivele măsuri de răspuns trebuie să permită organizației:

6.2.1. să declanșeze reacția la avertizările menționate la subpct. 6.1.2. prin activarea unor resurse și planuri de acțiune predefinite;

6.2.2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

6.2.3. să controleze modul de defectare al elementelor afectate definite la subpct. 3.1. IS.I.OR.205.

6.3. Organizația trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită organizației:

6.3.1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

6.3.2. să asigure atingerea unei stări de siguranță a elementelor afectate definite la subpct. 3.1. IS.I.OR.205 în timpul de redresare definit în prealabil de organizație.

7. IS.I.OR.225 Răspunsul la constatările notificate de AAC

7.1. După primirea notificării constatărilor de la AAC, organizația trebuie:

7.1.1. să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta;

7.1.2. să definească un plan de acțiuni corective;

7.1.3. să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către AAC.

7.2. Acțiunile menționate la subpct. 7.1. trebuie întreprinse în termenul convenit cu AAC.

8. IS.I.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor

8.1. Fără a aduce atingere reglementării aeronautice civilă „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la evenimentele de aviaţie civilă", aprobate prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020, organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite de AAC.

8.2. Fără a aduce atingere obligațiilor prevăzute în „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la evenimentele de aviaţie civilă", aprobate prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020, organizația trebuie să se asigure că orice incident sau vulnerabilitate în materie de securitate a informațiilor care poate reprezenta un risc semnificativ pentru siguranța aviației este raportată AAC. În plus:

8.2.1. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează o aeronavă ori un sistem sau o componentă asociată, organizația trebuie să raporteze acest lucru și titularului aprobării de proiect;

8.2.2. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează un sistem sau element constitutiv utilizat de organizație, ea trebuie să raporteze acest lucru organizației responsabile cu proiectarea sistemului sau a elementului constitutiv.

8.3. Organizația trebuie să raporteze situațiile menționate la subpct. 8.2. după cum urmează:

8.3.1. se transmite o notificare AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, de îndată ce organizația ia cunoștință de situație;

8.3.2. se transmite un raport AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, cât mai curând posibil, însă fără a depăși 72 de ore de la momentul în care organizația a luat cunoștință de situație, în afara cazului în care circumstanțe excepționale împiedică acest lucru.

Raportul se întocmește în forma definită de AAC și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația;

8.3.3. se transmite AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv un raport de urmărire în care se oferă detalii privind acțiunile întreprinse sau pe care organizația intenționează să le întreprindă în urma incidentului, precum și privind acțiunile pe care organizația intenționează să le întreprindă pentru a preveni, în viitor, producerea unor incidente similare de securitate a informațiilor.

Raportul de urmărire se transmite de îndată ce au fost identificate respectivele acțiuni și se întocmește în forma definită de AAC.

9. IS.I.OR.235 Subcontractarea activităților de management al securității informațiilor

9.1. Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la pct. 2. IS.I.OR.200, activitățile subcontractate respectă cerințele din prezentul Regulament și că organizația subcontractată lucrează sub supravegherea sa. Organizația trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

9.2. Organizația trebuie să se asigure că AAC poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul Regulament.

10. IS.I.OR.240 Cerințele în materie de personal

10.1. Managerul responsabil, desemnat în conformitate cu Regulamentul privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, cu Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană sau cu cadrul de reglementare pentru U-space, după caz, al organizațiile menționate la pct. 2 din prezentul Regulament trebuie să aibă drepturile statutare necesare pentru a se asigura că toate activitățile prevăzute în prezentul Regulament pot fi finanțate și efectuate. Persoana respectivă trebuie:

10.1.1. să se asigure că sunt disponibile toate resursele necesare pentru a se asigura conformitatea cu cerințele prezentului regulament;

10.1.2. să stabilească și să promoveze politica de securitate a informațiilor menționată la subpct. 2.1.1. IS.I.OR.200;

10.1.3. să demonstreze că are o înțelegere de bază a prezentului Regulament.

10.2. Managerul responsabil trebuie să numească o persoană sau un grup de persoane pentru a se asigura că organizația respectă cerințele prezentului regulament și trebuie să definească nivelul de autoritate al acestora. Persoana sau grupul de persoane au obligația să raporteze direct managerului responsabil și trebuie să dețină pregătirea, cunoștințele și experiența necesare îndeplinirii responsabilităților asumate. În cadrul procedurilor trebuie să se stabilească cine suplinește o anumită persoană în cazul unei absențe îndelungate a persoanei respective.

10.3. Managerul responsabil trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a conformității menționată la subpct. 2.1.12. IS.I.OR.200.

10.4. Atunci când organizația partajează structuri organizaționale, politici, procese și proceduri în materie de securitate a informațiilor cu alte organizații sau cu domenii ale propriei organizații care nu fac parte din aprobare sau din declarație, managerul responsabil își poate delega activitățile unei persoane responsabile comune.

Într-un astfel de caz, se stabilesc măsuri de coordonare între managerul responsabil al organizației și persoana responsabilă comună pentru a se asigura integrarea adecvată a managementului securității informațiilor în cadrul organizației.

10.5. Managerul responsabil sau persoana responsabilă comună menționată la subpct. 10.4. trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea pct. 2. IS.I.OR.200.

10.6. Organizația trebuie să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta Anexă.

10.7. Organizația trebuie să dispună de o procedură prin care să se asigure că personalul menționat la subpct. 10.6. are competența necesară pentru a-și îndeplini sarcinile.

10.8. Organizația trebuie să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.

10.9. Organizația trebuie să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului Regulament sunt stabilite în mod corespunzător.

11. IS.I.OR.245 Păstrarea evidențelor

11.1. Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor.

11.1.1. Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile:

11.1.1.1. orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor în conformitate cu subpct. 2.5. IS.I.OR.200;

11.1.1.2. contractele pentru activitățile menționate la subpct. 2.1.9. IS.I.OR.200;

11.1.1.3. evidențele proceselor-cheie menționate la subpct. 2.4. IS.I.OR.200;

11.1.1.4. evidențele riscurilor identificate în evaluarea riscurilor menționată la pct. 3. IS.I.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la pct. 4. IS.I.OR.210;

11.1.1.5. evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la pct. 5. IS.I.OR.215 și pct.8. IS.I.OR.230;

11.1.1.6. evidențele evenimentelor de securitate a informațiilor care ar fi necesare o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

11.1.2. Evidențele menționate la subpct. 11.1.1.1. se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea.

11.1.3. Evidențele menționate la subpct. 11.1.1.2. se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

11.1.4. Evidențele menționate la subpct. 11.1.1.3., subpct. 11.1.1.4. și subpct. 11.1.1.5. se păstrează timp de cel puțin cinci ani.

11.1.5. Evidențele menționate la subpct. 11.1.1.6. se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.

11.2. Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.

11.2.1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația.

11.2.2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, organizația trebuie să le furnizeze acestora, la părăsirea organizației, o copie a evidențelor personale.

11.3. Formatul evidențelor se specifică în procedurile organizației.

11.4. Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. Organizația trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

12. IS.I.OR.250 Manualul de management al securității informațiilor (MMSI)

12.1. Organizația trebuie să pună la dispoziția AAC un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și proceduri conexe la care se face trimitere în manualul respectiv, conținând:

12.1.1. o declarație semnată de managerul responsabil prin care se confirmă că organizația își va desfășura în permanență activitatea în conformitate cu prezenta Anexă și cu MMSI. Dacă managerul responsabil nu este directorul general al organizației, declarația trebuie să fie contrasemnată de directorul general;

12.1.2. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor definite la subpct. 10.2. și 10.3. IS.I.OR.240;

12.1.3. funcția, numele, atribuțiile, răspunderile, responsabilitățile și competența persoanei responsabile comune definite la subpct. 10.4. IS.I.OR.240, dacă este cazul;

12.1.4. politica de securitate a informațiilor instituită de organizație, astfel cum este menționată la subpct. 2.1.1. IS.I.OR.200;

12.1.5. o descriere generală a resurselor umane, din punctul de vedere al efectivelor și categoriilor, precum și a sistemului instituit pentru planificarea disponibilității personalului, astfel cum se prevede la pct. 10. IS.I.OR.240;

12.1.6. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea pct. 2. IS.I.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la subpct. 2.1.12. IS.I.OR.200;

12.1.7. o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpct. 12.1.2. și 12.1.6;

12.1.8. descrierea sistemului de raportare internă menționat la pct. 5. IS.I.OR.215;

12.1.9. procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular:

12.1.9.1. documentația menționată la subpct. 2.3. IS.I.OR.200;

12.1.9.2. procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la subpct. 2.1.9. IS.I.OR.200;

12.1.9.3. procedura de modificare a MMSI-ului, menționată la subpct.12.3.

12.1.10. informații detaliate referitoare la mijloace de conformare alternative aprobate în prezent.

12.2. Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de AAC. MMSI-ul trebuie modificat în funcție de necesități, astfel încât să reprezinte o descriere actualizată a SMSI-ului organizației. O copie a oricăror modificări aduse MMSI-ului trebuie transmisă AAC.

12.3. Modificările aduse MMSI-ului se gestionează în cadrul unei proceduri instituite de organizație. Orice modificare care nu este acoperită de domeniul de aplicare al acestei proceduri și orice modificare legată de modificările menționate la subpct. 13.2. IS.I.OR.255 trebuie să fie aprobată de AAC.

12.4. Organizația poate integra MMSI-ul în alte specificații sau manuale de management pe care le deține, cu condiția să existe o referință încrucișată clară indicând părțile din specificațiile sau manualul de management care corespund diferitelor cerințe cuprinse în prezenta Anexă.

13. IS.I.OR.255 Modificări ale sistemului de management al securității informațiilor

13.1. Modificările aduse SMSI-ului pot fi gestionate și notificate AAC în cadrul unei proceduri elaborate de organizație. Procedura respectivă trebuie să fie aprobată AAC.

13.2. În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la subpct. 13.1., organizația trebuie să solicite și să obțină o aprobare din partea AAC.

În ceea ce privește respectivele modificări:

13.2.1. cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite AAC să stabilească continuitatea conformității cu prezentul Regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia;

13.2.2. organizația trebuie să pună la dispoziția AAC toate informațiile solicitate pentru evaluarea modificării;

13.2.3. modificarea se implementează numai după primirea unei aprobări oficiale din partea AAC;

13.2.4. organizația trebuie să își desfășoare activitatea în condițiile stabilite de AAC în timpul implementării modificărilor respective.

14. IS.I.OR.260 Îmbunătățirea continuă

14.1. Organizația trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea SMSI-ului. Respectiva evaluare trebuie efectuată pe baza unui calendar predefinit de organizație sau în urma unui incident de securitate a informațiilor.

14.2. Dacă în urma evaluării efectuate în conformitate cu subpct. 14.1. se constată deficiențe, organizația trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să respecte cerințele aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, organizația trebuie să reevalueze elementele SMSI vizate de măsurile adoptate.

[PARTEA-IS.D.OR]

15. IS.D.OR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la pct. 2 subpct. 2.1. și subpct. 2.4. din prezentul Regulament.

16. IS.D.OR.200 Sistemul de management al securității informațiilor (SMSI)

16.1. Pentru a atinge obiectivele prevăzute la pct. 1 din Regulament, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația:

16.1.1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale organizației în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;

16.1.2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu pct. 17. IS.D.OR.205;

16.1.3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu pct. 18. IS.D.OR.210;

16.1.4. implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu pct. 19. IS.D.OR.215;

16.1.5. definește și implementează, în conformitate cu pct. 20. IS.D.OR.220, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, cu excepția cazurilor permise conform subpct. 17.4. IS.D.OR.205, asigură un răspuns la respectivele incidentele de securitate a informațiilor și de redresare în urma acestora;

16.1.6. implementează măsurile care au fost notificate de AAC ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației;

16.1.7. ia măsurile corespunzătoare, în conformitate cu pct. 21. IS.D.OR.225, pentru abordarea constatărilor notificate de AAC;

16.1.8. implementează un sistem de raportare externă în conformitate cu pct. 22. IS.D.OR.230, astfel încât AAC să poată lua măsuri corespunzătoare;

16.1.9. îndeplinește cerințele de la pct. 23. IS.D.OR.235 când subcontractează altor organizații orice parte a activităților menționate la pct. 16. IS.D.OR.200;

16.1.10. îndeplinește cerințele în materie de personal stabilite la pct. 24. IS.D.OR.240;

16.1.11. îndeplinește cerințele de păstrare a evidențelor stabilite la pct. 25. IS.D.OR.245;

16.1.12. monitorizează îndeplinirea de către organizație a cerințelor din prezentul Regulament și transmite managerului responsabil sau, în cazul organizațiilor de proiectare, șefului organizației de proiectare feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

16.1.13. protejează, fără a aduce atingere cerințelor aplicabile în materie de raportare a incidentelor, confidențialitatea oricăror informații pe care organizația le-ar fi putut primi de la alte organizații, în funcție de nivelul de sensibilitate a informațiilor respective.

16.2. Pentru a îndeplini în permanență cerințele menționate la pct. 1 din Regulament, organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu pct. 28. IS.D.OR.260.

16.3. Organizația trebuie să documenteze, în conformitate cu pct. 26. IS.D.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma subpct. 16.1. IS.D.OR.200 și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu pct. 27. IS.D.OR.255.

16.4. Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma subpct. 16.1. IS.D.OR.200 trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de organizație.

16.5. Fără a se aduce atingere obligației de conformitate cu cerințele de raportare prevăzute în reglementarea aeronautică civilă „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la evenimentele de aviaţie civilă”, aprobate prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020 și cu cerințele de la subpct. 16.1.13. IS.D.OR.200, organizația poate primi din partea AAC aprobarea de a nu implementa cerințele menționate la subpct. 16.1. - 16.4. și cerințele conexe prevăzute la pct. 17. IS.D.OR.205 – pct. 28. IS.D.OR.260, dacă demonstrează într-un mod considerat satisfăcător de AAC că activitățile, instalațiile și resursele sale, precum și serviciile pe care le operează, furnizează, primește și menține nu prezintă niciun risc în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației pentru organizația în sine sau pentru alte organizații. Aprobarea trebuie să se bazeze pe o evaluare documentată a riscurilor în materie de securitate a informațiilor, efectuată de organizație sau de o parte terță în conformitate cu pct. 17. IS.D.OR.205 și examinată și aprobată de AAC.

Menținerea valabilității respectivei aprobări va fi examinată de AAC în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.

17. IS.D.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor

17.1. Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă:

17.1.1. activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația;

17.1.2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpct. 17.1.1.

17.2. Organizația trebuie să identifice interfețele pe care le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

17.3. În ceea ce privește elementele și interfețele menționate la subpct. 17.1. și 17.2., organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie:

17.3.1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație;

17.3.2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu subpct. 17.1. și 17.2.

Clasificarea predefinită menționată la subpct. 17.3.1. trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Pe baza acestei clasificări și ținând cont dacă organizația dispune sau nu de un proces structurat și repetabil de management al riscurilor pentru operațiuni, organizația trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu pct. 18. IS.D.OR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în temeiul subpct. 17.3.1. se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la subpct. 17.2.

17.4. Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu subpct. 17.1., subpct.17.2. și subpct. 17.3. în oricare dintre următoarele situații:

17.4.1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

17.4.2. când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

17.4.3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

17.4.4. analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

18. IS.D.OR.210 Tratarea riscurilor în materie de securitate a informațiilor

18.1. Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu pct. 17. IS.D.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației:

18.1.1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

18.1.2. să diminueze consecințele asupra siguranței aviației, asociate materializării scenariului de amenințare;

18.1.3. să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

18.2. Persoana menționată la subpct. 24.1. și 24.2. IS.D.OR.240 și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu pct. 17. IS.D.OR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate.

Organizația trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu subpct. 17.2. IS.D.OR.205 cu privire la orice risc comun celor două organizații.

19. IS.D.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor

19.1. Organizația trebuie să instituie un sistem de raportare internă pentru a permite colectarea și evaluarea evenimentelor legate de securitatea informațiilor, inclusiv a celor care trebuie raportate în temeiul pct. 22. IS.D.OR.230.

19.2. Sistemul respectiv și procesul menționat la pct. 20. IS.D.OR.220 trebuie să îi permită organizației:

19.2.1. să identifice care dintre evenimentele raportate în temeiul subpct. 19.1. sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației;

19.2.2. să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpct. 19.2.1. și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu pct. 17. IS.D.OR.205 și pct. 20. IS.D.OR.220;

19.2.3. să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpct. 19.2.1;

19.2.4 să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.

19.3. Orice organizație subcontractată care ar putea expune organizația la riscuri în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației are obligația de a raporta organizației evenimentele de securitate a informațiilor. Rapoartele respective se transmit prin procedurile stabilite în angajamentele contractuale specifice și se evaluează în conformitate cu subpct. 19.2.

19.4. Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.

19.5. Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.

20. IS.D.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

20.1. În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu pct. 17. IS.D.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu pct. 18. IS.D.OR.210, organizația trebuie să implementeze măsuri de detectare a incidentelor și vulnerabilităților care indică materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită organizației:

20.1.1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

20.1.2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

20.2. Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu subpct. 20.1., care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Aceste măsuri de răspuns trebuie să permită organizației:

20.2.1. să declanșeze reacția la avertizările menționate la subpct. 20.1.2. prin activarea unor resurse și planuri de acțiune predefinite;

20.2.2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

20.2.3. să controleze modul de defectare al elementelor afectate definite la subpct. 17.1. IS.D.OR.205.

20.3. Organizația trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită organizației:

20.3.1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

20.3.2. să asigure atingerea unei stări de siguranță a elementelor afectate definite la subpct. 17.1. IS.D.OR.205 în timpul de redresare definit în prealabil de organizație.

21. IS.D.OR.225 Răspunsul la constatările notificate de AAC

21.1. După primirea notificării constatărilor de la AAC, organizația trebuie:

21.1.1. să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta;

21.1.2. să definească un plan de acțiuni corective;

21.1.3. să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către AAC.

21.2. Acțiunile menționate la subpct. 21.1. trebuie întreprinse în termenul convenit cu AAC.

22. IS.D.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor

22.1. Fără a aduce atingere prevederilor Reglementării aeronautice civile „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la

evenimentele de aviaţie civilă", aprobat prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020, organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite de AAC.

22.2. Fără a aduce atingere obligațiilor prevăzute în Reglementarea aeronautică civilă „Regulamentul privind raportarea, analiza şi acţiunile subsecvente cu privire la evenimentele de aviaţie civilă", aprobat prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020, organizația trebuie să se asigure că orice incident de securitate a informațiilor sau vulnerabilitate care poate reprezenta un risc semnificativ pentru siguranța aviației este raportată AAC. În plus:

22.2.1. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează o aeronavă ori un sistem sau o componentă asociată, organizația trebuie să raporteze acest lucru și titularului aprobării de proiect;

22.2.2. atunci când un astfel de incident sau o astfel de vulnerabilitate afectează un sistem sau element constitutiv utilizat de organizație, ea trebuie să raporteze acest lucru organizației responsabile cu proiectarea sistemului sau a elementului constitutiv.

22.3. Organizația trebuie să raporteze situațiile menționate la subpct. 22.2. după cum urmează:

22.3.1. se transmite o notificare AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, de îndată ce organizația ia cunoștință de situație;

22.3.2. se transmite un raport AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, cât mai curând posibil, însă fără a depăși 72 de ore de la momentul în care organizația a luat cunoștință de situație, în afara cazului în care circumstanțe excepționale împiedică acest lucru.

Raportul se întocmește în forma definită de AAC și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația;

22.3.3. se transmite AAC și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv un raport de urmărire în care se oferă detalii privind acțiunile întreprinse sau pe care organizația intenționează să le întreprindă în urma incidentului, precum și privind acțiunile pe care organizația intenționează să le întreprindă pentru a preveni, în viitor, producerea unor incidente similare de securitate a informațiilor.

Raportul de urmărire se transmite de îndată ce au fost identificate respectivele acțiuni și se întocmește în forma definită de AAC.

23. IS.D.OR.235 Subcontractarea activităților de management al securității informațiilor

23.1. Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la pct. 20. IS.D.OR.200, activitățile subcontractate respectă cerințele din prezentul Regulament și că organizația subcontractată lucrează sub supravegherea sa. Organizația trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

23.2. Organizația trebuie să se asigure că AAC poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul Regulament.

24. IS.D.OR.240 Cerințele în materie de personal

24.1. Managerul responsabil al organizației sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare, desemnat în conformitate cu Regulamentele aprobate prin Hotărârea de Guvern nr. 91/2024 și respectiv Hotărârea de Guvern nr. 653/2018, astfel cum se menționează la prevederile pct. 2 subpct. 2.1 și 2.4 din prezentul Regulament, trebuie să aibă drepturile statutare necesare pentru a se asigura că toate activitățile prevăzute în prezentul Regulament pot fi finanțate și efectuate. Persoana respectivă trebuie:

24.1.1. să se asigure că sunt disponibile toate resursele necesare pentru a se conforma cerințelor prezentului Regulament;

24.1.2. să stabilească și să promoveze politica de securitate a informațiilor menționată la subpct. 16.1.1. IS.D.OR.200;

24.1.3. să demonstreze că deține cunoștințe de bază privind prezentul Regulament.

24.2. Managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare trebuie să numească o persoană sau un grup de persoane pentru a asigura conformitatea organizației cu cerințele prezentului Regulament și trebuie să definească nivelul de autoritate al acestora. Persoana sau grupul de persoane au obligația să raporteze direct managerului responsabil sau, în cazul organizațiilor de proiectare, șefului organizației de proiectare și trebuie să dețină pregătirea, cunoștințele și experiența necesare executării responsabilităților asumate. În cadrul procedurilor trebuie să se stabilească cine suplinește o anumită persoană în cazul unei absențe îndelungate a persoanei respective.

24.3. Managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a conformității menționată la subpct. 16.1.12. IS.D.OR.200.

24.4. Atunci când organizația partajează structuri organizaționale, politici, procese și proceduri în materie de securitate a informațiilor cu alte organizații sau cu domenii ale propriei organizări care nu fac parte din aprobare sau din declarație, managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare, își poate delega activitățile unei persoane responsabile comune.

Într-un astfel de caz, se stabilesc măsuri de coordonare între managerul responsabil al organizației sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare și persoana responsabilă comună pentru a se asigura integrarea adecvată a managementului securității informațiilor în cadrul organizației.

24.5. Managerul responsabil sau șeful organizației de proiectare ori persoana responsabilă comună menționată la subpct. 24.4. trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea pct.16. IS.D.OR.200.

24.6. Organizația trebuie să dispună de un proces prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta Anexă.

24.7. Organizația trebuie să dispună de un proces prin care să se asigure că personalul menționat la subpct. 24.6. are competența necesară pentru a-și îndeplini sarcinile.

24.8. Organizația trebuie să dispună de un proces prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.

24.9. Organizația trebuie să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului regulament sunt stabilite în mod corespunzător.

25. IS.D.OR.245 Păstrarea evidențelor

25.1. Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor.

25.1.1. Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile:

25.1.1.1. orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor în conformitate cu subpct. 16.5. IS.D.OR.200;

25.1.1.2. contractele pentru activitățile menționate la subpct. 16.1.9. IS.D.OR.200;

25.1.1.3. evidențele proceselor-cheie menționate la subpct. 16.4. IS.D.OR.200;

25.1.1.4. evidențele riscurilor identificate în evaluarea riscurilor menționată la pct. 17. IS.D.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la pct. 18. IS.D.OR.210;

25.1.1.5. evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la pct. 19. IS.D.OR.215 și pct. 22. IS.D.OR.230;

25.1.1.6. evidențele evenimentelor de securitate a informațiilor care ar putea necesita o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

25.1.2. Evidențele menționate la subpct. 25.1.1.1. se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea.

25.1.3. Evidențele menționate la subpct. 25.1.1.2. se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

25.1.4. Evidențele menționate la subpct. 25.1.1.3., subpct. 25.1.1.4. și subpct. 25.1.1.5. se păstrează timp de cel puțin cinci ani.

25.1.5. Evidențele menționate la subpct. 25.1.1.6. se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.

25.2. Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.

25.2.1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația.

25.2.2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, organizația trebuie să le furnizeze acestora, la părăsirea organizației, o copie a evidențelor personale.

25.3. Formatul evidențelor se specifică în procedurile organizației.

25.4. Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. Organizația trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

26. IS.D.OR.250 Manualul de management al securității informațiilor (MMSI)

26.1. Organizația trebuie să pună la dispoziția AAC un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și proceduri conexe la care se face trimitere în manualul respectiv, conținând:

26.1.1. o declarație semnată de managerul responsabil sau, în cazul organizațiilor de proiectare, de șeful organizației de proiectare, prin care se confirmă că organizația își va desfășura în permanență activitatea în conformitate cu prezenta anexă și cu MMSI. Dacă managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare nu este directorul general al organizației, declarația trebuie să fie contrasemnată de directorul general;

26.1.2. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor menționate la subpct. 24.2. și subpct. 24.3. IS.D.OR.240;

26.1.3. funcția, numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei responsabile comune menționate la subpct. 24.4. IS.D.OR.240, dacă este cazul;

26.1.4. politica de securitate a informațiilor instituită de organizație, astfel cum este menționată la subpct. 16.1.1. IS.D.OR.200;

26.1.5. o descriere generală a resurselor umane, din punctul de vedere al efectivelor și categoriilor, precum și a sistemului instituit pentru planificarea disponibilității personalului, astfel cum se prevede la subpct. 24.4. IS.D.OR.240;

26.1.6. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea pct. 16. IS.D.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la subpct. 16.1.12. IS.D.OR.200;

26.1.7. o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpct. 26.1.2. și subpct. 26.1.6.;

26.1.8. descrierea sistemului de raportare internă menționat la pct. 19. IS.D.OR.215;

26.1.9. procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular:

26.1.9.1. documentația menționată la subpct. 16.3. IS.D.OR.200;

26.1.9.2. procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la subpct. 16.1.9. IS.D.OR.200;

26.1.9.3. procedura de modificare a MMSI-ului, definită la subpct. 26.3.

26.1.10. informații detaliate referitoare la mijloace alternative de punere în conformitate *(AltMoC)* aprobate în prezent.

26.2. Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de AAC. MMSI-ul trebuie modificat în funcție de necesități, astfel încât să reprezinte o descriere actualizată a SMSI-ului organizației. O copie a oricăror modificări aduse MMSI-ului trebuie transmisă AAC.

26.3. Modificările aduse MMSI-ului se gestionează în cadrul unei proceduri instituite de organizație. Orice modificare care nu este acoperită de domeniul de aplicare al acestei proceduri și orice modificare legată de modificările menționate la subpct. 27.2. IS.D.OR.255 trebuie să fie aprobată de AAC.

26.4. Organizația poate integra MMSI-ul în alte specificații sau manuale de management pe care le deține, cu condiția să existe o referință încrucișată clară indicând părțile din specificațiile sau manualul de management care corespund diferitelor cerințe cuprinse în prezenta Anexă.

27. IS.D.OR.255 Modificări ale sistemului de management al securității informațiilor

27.1. Modificările aduse SMSI-ului pot fi gestionate și notificate AAC în cadrul unei proceduri elaborate de organizație. Procedură respectivă trebuie să fie aprobată de AAC.

27.2. În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la subpct. 27.1., organizația trebuie să solicite și să obțină o aprobare din partea AAC.

În ceea ce privește aceste modificări:

27.2.1. cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite AAC să stabilească continuitatea conformității cu prezentul Regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia;

27.2.2. organizația trebuie să pună la dispoziția AAC toate informațiile solicitate pentru evaluarea modificării;

27.2.3. modificarea se implementează numai după primirea unei aprobări oficiale din partea AAC;

27.2.4. organizația trebuie să își desfășoare activitatea în condițiile stabilite de AAC în timpul implementării modificărilor respective.

28. IS.D.OR.260 Îmbunătățirea continuă

28.1. Organizația trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea SMSI-ului. Respectiva evaluare trebuie efectuată pe baza unui calendar predefinit de organizație sau în urma unui incident de securitate a informațiilor.

28.2. Dacă în urma evaluării efectuate în conformitate cu subpct. 28.1. se constată deficiențe, organizația trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să se conformeze cerințelor aplicabile și că el menține riscurile în

materie de securitate a informațiilor la un nivel acceptabil. În plus, organizația trebuie să reevalueze elementele SMSI vizate de măsurile adoptate.

Anexa nr. 2
la Hotărârea Guvernului nr.___/2025

MODIFICĂRILE
ce se operează în unele hotărâri ale Guvernului

1. Regulamentul privind stabilirea cerinţelor şi procedurilor administrative de certificare pentru navigabilitate şi mediu sau declaraţia de conformitate a aeronavelor şi a produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, aprobat prin Hotărârea de Guvern nr. 91/2024 (Monitorul Oficial al Republicii Moldova, 2024, nr. 118-121, art.272), se modifică după cum urmează:

1.1. La Anexa nr. 1 PARTEA 21 CERTIFICAREA AERONAVELOR ȘI A PRODUSELOR, PIESELOR ȘI ECHIPAMENTELOR AFERENTE, PRECUM ȘI A ORGANIZAȚIILOR DE PROIECTARE ȘI DE PRODUCȚIE, după punctul 21.A.139 se completează cu punctul 21.A.139A:

„**21.A.139A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management al producției prevăzut la pct. 21.A.139, organizația de producție instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

1.2. După punctul 21.A.239 se completează cu punctul 21.A.239A:

„**21.A.239A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management al proiectării prevăzut la pct. 21.A.239, organizația de proiectare instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

1.3. Se modifică titlul punctului 21.B.30:

„**21.B.30 Atribuirea de sarcini**”;

1.4. Pct. 21.B.15 se completează cu lit. (c):

„**21.B.15 Informarea**

(c) AAC furnizează Agenției Securitate Cibernetică cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. 22. IS.D.OR.230 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”

1.5. După punctul 21.B.20 se completează cu punctul 21.B.20A cu următorul text:

„**21.B.20A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. 21.B.15 lit. (c) și pentru furnizarea fără întârzieri nejustificate Agenției pentru Securitate Cibernetică a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri în egală măsură Agenției pentru Securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”

1.6. Punctul 21.B.25 se completează cu litera (e):

„**21.B.25 Sistemul de management**

(e) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte Anexa nr. 1 (partea IS.AR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”

1.7. Punctul 21.B.30 Atribuirea de sarcini se completează cu lit. (c):

„**21.B.30 Atribuirea de sarcini**

(c) Pentru certificarea și supravegherea conformității organizației cu pct. 21.A.139A și 21.A.239A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. 21.B.25 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său."

1.8. Punctul 21.B.221 se completează cu lit. (g):

„**21.B.221 Principiile de supraveghere**

(g) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. 21.A.139A, în plus față de respectarea dispozițiilor de la lit. (a)-(f), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 din Anexa nr. 2 la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației."

1.9. După punctul 21.B.240 se completează cu punctul 21.B.240A:

„ **21.B.240A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 27.1. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, AAC include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. 21.B.221. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. 21.B.225.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu subpct. 27.2. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviație:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea."

1.10. Punctul 21.B.431 se completează cu litera (d):

„**21.B.431 Principiile de supraveghere**

(d) Pentru certificarea și supravegherea conformității organizației cu pct. 21.A.239A, în plus față de respectarea dispozițiilor de la lit. (a)-(c), AAC respectă următoarele principii:

1. examinează interfețele și riscurile asociate identificate în conformitate cu subpct. 17.2. IS.D.OR.205 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviație, de fiecare organizație care face obiectul supravegherii sale;

2. dacă se constată discrepanțe în interfețele reciproce și riscurile asociate identificate de diferite organizații, AAC le examinează împreună cu organizațiile vizate și, dacă este necesar, formulează constatări corespunzătoare pentru a asigura implementarea de măsuri corective;

3. dacă din examinarea documentației, efectuată în temeiul subpct. 2, reiese că există riscuri semnificative asociate interfețelor cu organizații supravegheate de altă autoritate competentă, aceste informații se comunică autorității corespunzătoare."

1.11. După punctul 21.B.435 se completează cu punctul 21.B.435A:

„ **21.B.435A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 27.1. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviație, AAC include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. 21.B.431. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. 21.B.433.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu pct. subpct. 27.2. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviație:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.".

2. Regulamentul privind procedurile administrative referitoare la aerodromuri, aprobat prin Hotărârea de Guvern nr. 653/2018 (Monitorul Oficial al Republicii Moldova, 2018, nr. 256-265, art.713), cu modificările ulterioare, se modifică după cum urmează:

2.1. La Anexa nr. 2 CERINȚE APLICABILE ORGANIZAȚIILOR (ADR.OR), după pct. ADR.OR.D.005 se completează cu punctul ADR.OR.D.005A:

„**ADR.OR.D.005A Sistemul de management al securității informațiilor**

Operatorul de aerodrom/aeroport instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura

managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”.

2.2. Punctul ADR.OR.D.007 se modifică:

„**ADR.OR.D.007 Managementul datelor aeronautice și al informațiilor aeronautice**

(a) În cadrul sistemului său de management, operatorul de aerodrom/aeroport implementează și menține un sistem de management al calității care cuprinde următoarele activități:

(1) activitățile sale legate de datele aeronautice;

(2) activitățile sale de furnizare de informații aeronautice.

(b) În cadrul sistemului său de management, operatorul de aerodrom/aeroport stabilește un sistem de management al securității pentru a asigura securitatea datelor operaționale pe care le primește, le generează sau le utilizează în alt mod, astfel încât accesul la respectivele date operaționale să fie limitat numai la persoanele autorizate.

(c) Sistemul de management al securității trebuie să definească următoarele elemente:

(1) procedurile referitoare la evaluarea și reducerea riscurilor de securitate a datelor, monitorizarea și îmbunătățirea securității, examinările de securitate și diseminarea rezultatelor;

(2) mijloacele destinate să detecteze breșele de securitate și să alerteze personalul prin avertizări adecvate cu privire la securitate;

(3) mijloacele de control al efectelor cauzate de breșele de securitate și de identificare a măsurilor de remediere și a procedurilor de reducere a riscurilor pentru prevenirea repetării acestora.

(d) Operatorul de aerodrom/aeroport asigură autorizarea de securitate a personalului său în ceea ce privește securitatea datelor aeronautice.

(e) Aspectele legate de securitatea informațiilor trebuie gestionate în conformitate cu pct. ADR.OR.D.005A.”.

2.3. După punctul ADR.OR.F.045 se completează cu punctul ADR.OR.F.045A:

„**ADR.OR.F.045A Sistemul de management al securității informațiilor**

Organizația responsabilă cu furnizarea de AMS instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”.

2.4. După punctul ADR.AR.A.015 se completează cu punctul ADR.AR.A.025 Informarea:

„ **ADR.AR.A.025 Informarea**

(a) AAC informează, fără întârzieri nejustificate, organul central de specialitate în domeniul aviației civile în cazul oricăror probleme semnificative legate de punerea în aplicare a prevederilor Codului aerian și a normelor sale de punere în aplicare.

(b) Autoritatea responsabilă de investigarea incidentelor și accidentelor furnizează AAC informații semnificative din punctul de vedere al siguranței, provenite din rapoartele pe care le-a primit cu privire la evenimente.

(c) AAC furnizează cât mai repede posibil Agenției pentru Securitate Cibernetică informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. IS.D.OR.230 din anexa nr. 2 (partea IS.D.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.";

2.5. După punctul ADR.AR.A.030 se completează cu punctul ADR.AR.A.030A:

„**ADR.AR.A.030A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. ADR.AR.A.025 lit. (c) și pentru furnizarea fără întârzieri nejustificate Agenției pentru Securitate Cibernetică a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul prevederilor Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri în egală măsură Agenției pentru Securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate."

2.6. Punctul ADR.AR.B.005 se adaugă lit. (d):

„**ADR.AR.B.005 Sistemul de management**

(d) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte Anexa nr. 1 (partea IS.AR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."

2.7. Se completează cu punctul ADR.AR.B.010 Atribuirea de sarcini:

„**ADR.AR.B.010 Atribuirea de sarcini**

(a) AAC atribuie numai entităților calificate sarcini legate de certificarea inițială sau de supravegherea continuă a persoanelor sau a organizațiilor care fac obiectul Codului aerian și al normelor sale de punere în aplicare. Atunci când atribuie sarcini, AAC se asigură că:

1. dispune de un sistem pentru evaluarea inițială și continuă a conformității entității calificate în conformitate cu prevederile Codului aerian.

Sistemul și rezultatele evaluării se documentează;

2. a încheiat un acord documentat cu entitatea calificată, aprobat de ambele părți la nivelul de conducere corespunzător, care definește în mod clar:

(i) sarcinile care trebuie executate;

(ii) declarațiile, rapoartele și înregistrările care trebuie furnizate;

(iii) condițiile tehnice care trebuie îndeplinite la executarea unor astfel de sarcini;

(iv) acoperirea responsabilității asociate; și

(v) protecția acordată informațiilor obținute în cursul executării unor astfel de sarcini.

(b) AAC se asigură că procesul de audit intern și procesul de management al riscurilor de siguranță impuse de pct. ADR.AR.B.005 lit. (a) pct. 4) vizează toate sarcinile de certificare sau de supraveghere continuă executate în numele său.

(c) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ADR.OR.D.005A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. ADR.AR.B.005 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”

2.8. Punctul ADR.AR.C.005 se completează cu litera (f):

„**ADR.AR.C.005 Supraveghere**

(f) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ADR.OR.D.005A, în plus față de respectarea dispozițiilor de la lit. (a)-(e), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau al subpct. 16.5. IS.D.OR.200 din Anexa nr. 2 la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”

2.9. După punctul ADR.AR.C.040 se completează cu punctul ADR.AR.C.040A:

„ **ADR.AR.C.040A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 27.1. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la

Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, AAC include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. ADR.AR.C.005. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. ADR.AR.C.055.

(b) În privința altor modificări care necesită o cerere de aprobare în conformitate cu subpct. 27.2. IS.D.OR.255 din Anexa nr. 2 (partea IS.D.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”

3. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, aprobat prin Hotărârea de Guvern nr. 204/2020 (Monitorul Oficial al Republicii Moldova, 2020, nr. 165-176, art.552), cu modificările ulterioare, se modifică după cum urmează:

3.1. Anexa nr. 6 CERINŢE APLICABILE AUTORITĂŢII AERONAUTICE CIVILE [PARTEA ARA] se completează cu punctul ARA.GEN.125 lit. (c):

„**ARA.GEN.125 Informarea**

(c) AAC furnizează Agenției pentru Securitate Cibernetică cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. 8. IS.I.OR.230 din Anexa nr.2 la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.”;

3.2. După punctul ARA.GEN.135 se completează cu punctul ARA.GEN.135A:

„**ARA.GEN.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. ARA.GEN.125 lit. (c) și pentru furnizarea fără întârzieri nejustificate către Agenția pentru Securitate Cibernetică, informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra

siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri Agenției pentru Securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”;

3.3. Punctul ARA.GEN.200 se completează cu lit. (e):

„**ARA.GEN.200 Sistemul de management**

(e) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte prevederile Anexei nr. 1 (partea IS.AR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

3.4. După punctul ARA.GEN.200 se completează cu punctul ARA.GEN.205:

„**ARA.GEN.205 Atribuirea de sarcini**

(a) AAC poate atribuie sarcini legate de certificarea inițială sau de supravegherea continuă a persoanelor sau organizațiilor care fac obiectul Codului aerian și al normelor sale de aplicare numai entităților calificate. Atunci când atribuie sarcini, AAC se asigură că:

1. dispune de un sistem pentru evaluarea inițială și continuă a conformității entității calificate în conformitate cu Codul aerian. Acest sistem și rezultatele evaluării trebuie să fie documentate;

2. a încheiat un acord documentat cu entitatea calificată, aprobat de ambele părți la nivelul de conducere corespunzător, care definește în mod clar:

(i) sarcinile care urmează a fi executate;

(ii) declarațiile, rapoartele și înregistrările care trebuie furnizate;

(iii) condițiile tehnice care trebuie îndeplinite la executarea unor astfel de sarcini;

(iv) asigurarea corespunzătoare a răspunderii; și

(v) protecția acordată informațiilor obținute în cursul exercitării unor astfel de sarcini.

(b) AAC se asigură că procesul de audit intern și procesul de management al riscurilor de siguranță impuse de pct. ARA.GEN.200 lit. (a) pct. 4 cuprind toate sarcinile de certificare sau de supraveghere continuă executate în numele său.

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ORA.GEN.200A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. ARA.GEN.200 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;

3.5. Punctul ARA.GEN.300 se completează cu lit. (g):

„**ARA.GEN.300 Supravegherea**

(g) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ORA.GEN.200A, în plus față de respectarea dispozițiilor de la lit. (a)-(e), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau al subpct. 16.5. IS.D.OR.200 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;

3.6. După punctul ARA.GEN.330 se completează cu punctul ARA.GEN.330A Modificări ale sistemului de management al securității informațiilor:

„**ARA.GEN.330A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct.13.1. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, AAC include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. ARA.GEN.300. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. ARA.GEN.350.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu subpct. 13.2. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”;

3.7. Anexa nr. 7 CERINŢE APLICABILE ORGANIZAŢIILOR PENTRU PERSONALUL NAVIGANT [PARTEA ORA], se completează cu punctul ORA.GEN.200A:

„**ORA.GEN.200A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la pct. ORA.GEN.200, organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind cerințele referitoare la managementul riscurilor

în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”

4. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, aprobat prin Hotărârea de Guvern nr. 612/2022, (Monitorul Oficial al Republicii Moldova, 2022, nr. 363-373, art.868), cu modificările ulterioare, se modifică după cum urmează:

4.1. La Anexa nr. 2 CERINŢE APLICABILE AUTORITĂŢII AERONAUTICE CIVILE PENTRU OPERAŢIUNILE AERIENE (Partea ARO), după punctul ARO.GEN.120 se completează cu punctul ARO.GEN.125:

„**ARO.GEN.125 Informarea**

(a) AAC, informează organul central de specialitate în domeniul aviației civile, fără întârzieri nejustificate, în cazul apariției oricăror probleme semnificative legate de implementarea a Codului aerian și a normelor sale de aplicare.

(b) Autoritatea responsabilă de investigarea incidentelor și accidentelor furnizează AAC informații semnificative din punctul de vedere al siguranței, provenite din rapoartele pe care le-a primit cu privire la evenimente.

(c) AAC furnizează cât mai repede posibil Agenției pentru Securitatea Cibernetică, informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. 8. IS.I.OR.230 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.”;

4.2. După punctul ARO.GEN.135 se completează cu punctul ARO.GEN.135A cu următorul text:

„**ARO.GEN.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. ARO.GEN.125 lit. (c) și pentru furnizarea fără întârzieri nejustificate către Agenția pentru Securitate Cibernetică a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri în egală măsură Agenției pentru Securitatea Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”;

4.3. Punctul ARO.GEN.200 se completează cu lit. (e):

„**ARO.GEN.200 Sistemul de management**

(e) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte Anexa nr. 1 (partea IS.AR) la Regulamentul privind cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

4.4. Se completează cu punctul ARO.GEN.205 Atribuirea de sarcini:

„ **ARO.GEN.205 Atribuirea de sarcini**

(a) AAC poate atribui sarcini legate de certificarea inițială, de autorizarea pentru operațiuni specializate sau de supravegherea continuă a persoanelor sau organizațiilor care fac obiectul Codului aerian și al normelor sale de punere în aplicare numai entităților calificate. Atunci când atribuie sarcini, AAC se asigură că:

1. dispune de un sistem pentru evaluarea inițială și continuă a conformității entității calificate cu prevederile Codului aerian.

Sistemul și rezultatele evaluării se documentează;

2. a încheiat un acord documentat cu entitatea calificată, aprobat de ambele părți la nivelul de conducere corespunzător, care definește în mod clar:

(i) sarcinile care urmează a fi executate;

(ii) declarațiile, rapoartele și înregistrările care trebuie furnizate;

(iii) condițiile tehnice care trebuie îndeplinite la executarea unor astfel de sarcini;

(iv) asigurarea corespunzătoare a răspunderii; și

(v) protecția acordată informațiilor obținute în cursul exercitării unor astfel de sarcini.

(b) AAC se asigură că procesul de audit intern și procesul de management al riscurilor de siguranță impuse de pct. ARO.GEN.200 lit. (a) pct. 4 vizează toate sarcinile de certificare, de autorizare sau de supraveghere continuă executate în numele său.

„(c) Pentru certificarea și supravegherea conformității organizației cu pct. ORO.GEN.200A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. ARO.GEN.200 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;

4.5. Punctul ARO.GEN.300 se completează cu lit. (g):

„**ARO.GEN.300 Supravegherea**

(g) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ORO.GEN.200A, în plus față de respectarea dispozițiilor de la lit. (a)-(f), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau subpct. 16.5. IS.D.OR.200 din Anexa nr. 2 la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;

4.6. după punctul ARO.GEN.330 se completează cu punctul ARO.GEN.330A:

„**ARO.GEN.330A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 13.1. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, AAC include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. ARO.GEN.300. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. ARO.GEN.350.

(b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu subpct. 13.2. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”

4.7. La anexa nr. 3 CERINŢE APLICABILE ORGANIZAŢIILOR PENTRU EFECTUAREA OPERAŢIUNILOR AERIENE (Partea ORO), după punctul ORO.GEN.200 se completează cu punctul ORO.GEN.200A:

„**ORO.GEN.200A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la pct. ORO.GEN.200, operatorul instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației,

pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”

5. Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, aprobat prin Hotărârea de Guvern nr. 134/2019 (Monitorul Oficial al Republicii Moldova, 2019, nr. 94-99, art.190), se modifică după cum urmează:

5.1. La Anexa nr. 1 PARTEA ATCO.AR – CERINŢE APLICABILE AUTORITĂŢII AERONAUTICE CIVILE, după punctul ATCO.AR.A.015, se completează cu punctul ATCO.AR.A.020:

„ **ATCO.AR.A.020 Informarea**

(a) AAC trebuie să informeze organul central de specialitate în domeniul aviației civile în cazul oricăror probleme semnificative legate de punerea în aplicare a prevederilor Codului aerian și a actelor sale de punere în aplicare.

(b) Fără a aduce atingere Regulamentului privind raportarea, analiza și acțiunile subsecvente cu privire la evenimentele de aviație civilă, aprobat prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020 și actelor sale de punere în aplicare, AAC trebuie să furnizeze Agenției pentru Securitate Cibernetică cât mai curând posibil informațiile semnificative din punctul de vedere al siguranței care reies din rapoartele cu privire la evenimente stocate în baza sa de date națională.

(c) AAC furnizează Agenției pentru Securitate Cibernetică cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. 8. IS.I.OR.230 din Anexa nr. 2 (partea IS.I.OR) la la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.”

5.2. După punctul ATCO.AR.A.025 se completează cu punctul ATCO.AR.A.025A:

„**ATCO.AR.A.025A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. ATCO.AR.A.020 și pentru furnizarea fără întârzieri nejustificate către Agenția pentru securitate Cibernetică a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri în egală măsură Agenției pentru securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”;

5.3. Punctul ATCO.AR.B.001 se completează cu litera (e):

„**ATCO.AR.B.001 Sistemul de management**

(e) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte Anexa nr. 1 (partea IS.AR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

5.4. După punctul ATCO.AR.B.001 se completează cu punctul ATCO.AR.B.005:

„**ATCO.AR.B.005 Atribuirea de sarcini**

(a) În cazul în care AAC atribuie sarcini legate de certificarea inițială sau de supravegherea continuă a persoanelor sau a organizațiilor care fac obiectul Codului aerian și al actelor sale de punere în aplicare, respectivele sarcini trebuie atribuite exclusiv unor entități calificate. Atunci când atribuie sarcini, AAC se asigură că:

1. dispune de un sistem pentru evaluarea inițială și continuă a conformității entității calificate în conformitate cu prevederile Codului aerian.

Acest sistem și rezultatele evaluării trebuie să fie documentate;

2. a încheiat un acord documentat cu o entitate calificată, aprobat de ambele părți la nivelul de conducere corespunzător, care definește în mod clar:

(i) sarcinile care trebuie executate;

(ii) declarațiile, rapoartele și evidențele care trebuie furnizate;

(iii) condițiile tehnice care trebuie îndeplinite la executarea sarcinilor respective;

(iv) acoperirea responsabilității asociate; precum și

(v) protecția acordată informațiilor obținute în cursul executării unor astfel de sarcini.

(b) AAC se asigură că procesul de audit intern și procesul de management al riscurilor de siguranță impuse de pct. ATCO.AR.B.001 lit. (a) pct. 4 cuprind toate sarcinile de certificare sau de supraveghere executate în numele său.

c) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ATCO.OR.C.001A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea națională relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea națională relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. ATCO.AR.B.001 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său."

5.5. Punctul ATCO.AR.C.001 se completează cu litera (f):

„**ATCO.AR.C.001 Supravegherea**

(f) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ATCO.OR.C.001A, în plus față de respectarea dispozițiilor de la literele (a)-(e), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau al subpct. 16.5. IS.D.OR.200 din Anexa nr. 2 la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.";

5.6. După punctul ATCO.AR.E.010 se completează cu punctul ATCO.AR.E.010A:

„**ATCO.AR.E.010A Modificări ale sistemului de management al securității informațiilor**

(a) În ceea ce privește modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 13.1. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației, AAC include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. ATCO.AR.C.001. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. ATCO.AR.C.010.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu subpct. 13.2. IS.I.OR.255 din Anexa nr.2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea."

5.7. La Anexa nr. 2 PARTEA ATCO.OR – CERINŢE PENTRU ORGANIZAŢIILE

DE PREGĂTIRE A CONTROLORILOR DE TRAFIC AERIAN ŞI PENTRU CENTRELE DE MEDICINĂ AERONAUTICĂ, după punctul ATCO.OR.C.001 se completează cu punctul ATCO.OR.C.001A:

„**ATCO.OR.C.001A Sistemul de management al securității informațiilor**

Pe lângă sistemul de management menționat la pct. ATCO.OR.C.001, organizația de pregătire instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”

6. Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, aprobat prin Hotărârea de Guvern nr. 119/2023 (Monitorul Oficial al Republicii Moldova, 2023, nr. 141-144, art.309), cu modificările ulterioare, se modifică după cum urmează:

6.1. La anexa nr. 2 CERINȚE APLICABILE AUTORITĂȚILOR COMPETENTE — SUPRAVEGHEREA SERVICIILOR ȘI A ALTOR FUNCȚII ALE REȚELEI ATM (partea

ATM/ANS.AR), după punctul ATM/ANS.AR.A.015 se completează cu punctul ATM/ANS.AR.A.020:

„**ATM/ANS.AR.A.020 Informarea**

(a) AAC trebuie să notifice organul central de specialitate în domeniul aviației civile fără întârzieri nejustificate orice probleme semnificative legate de punerea în aplicare a dispozițiilor Codului aerian și a actelor de punere în aplicare.

(b) Fără a aduce atingere Regulamentul privind raportarea, analiza și acțiunile subsecvente cu privire la evenimentele de aviație civilă, aprobat prin Ordinul Ministerului Infrastructurii și Dezvoltării Regionale nr. 119/2020 și al actelor sale de punere în aplicare, AAC trebuie să furnizeze autorității responsabile de investigarea incidentelor și accidentelor aeronautice cât mai curând posibil informațiile semnificative din punctul de vedere al siguranței care reies din rapoartele cu privire la evenimente stocate în baza sa de date națională.

(c) AAC furnizează Agenției pentru Securitate Cibernetică cât mai repede posibil informațiile semnificative din punctul de vedere al siguranței provenite din rapoartele de securitate a informațiilor pe care le-a primit în temeiul pct. 8. IS.I.OR.230 din Anexa nr. 2 (partea IS.I.OR) Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.”;

6.2. După punctul ATM/ANS.AR.A.025 se completează cu punctul ATM/ANS.AR.A.025A:

„ **ATM/ANS.AR.A.025A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**

(a) AAC implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate

națională relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare.

(b) AAC implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu pct. ATM/ANS.AR.A.020 lit. (c) și pentru furnizarea fără întârzieri nejustificate către Agenția pentru Securitate Aeronautică a oricăror informații, inclusiv recomandări sau măsuri corective de întreprins, necesare pentru ca acestea să reacționeze în timp util la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Codului aerian și ale actelor sale de punere în aplicare.

(c) La primirea informațiilor menționate la lit. (a) și (b), AAC ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației.

(d) Măsurile luate în conformitate cu lit. (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Codului aerian și al actelor sale de punere în aplicare. AAC notifică aceste măsuri în egală măsură Agenției pentru Securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”;

6.3. Punctul ATM/ANS.AR.B.001 se completează cu litera (e):

„**ATM/ANS.AR.B.001 Sistemul de management**

(e) În plus față de cerințele de la lit. (a), sistemul de management instituit și menținut de AAC trebuie să respecte Anexa nr.1 (partea IS.AR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

6.4. Titlul punctului ATM/ANS.AR.B.005 se modifică, și se completează cu lit. (c):

„**ATM/ANS.AR.B.005 Atribuirea de sarcini**

(ii) se adaugă lit. (c) cu următorul text:

„(c) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ATM/ ANS.OR.B.005A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea cibernetică. Atunci când atribuie sarcini, AAC se asigură că:

1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea națională relevantă;

2. rezultatele activităților de certificare și de supraveghere desfășurate de entitatea calificată sau de autoritatea națională relevantă sunt integrate în dosarele generale de certificare și de supraveghere ale organizației;

3. propriul sistem de management al securității informațiilor, instituit în conformitate cu pct. ATM/ANS.AR.B.001 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;

6.5. punctul ATM/ANS.AR.C.010 se completează cu litera (d):

„**ATM/ANS.AR.C.010 Supraveghere**

(d) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. ATM/ANS.OR.B.005A, în plus față de respectarea dispozițiilor de la lit. (a)-(c), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau al subpct. 16.5. IS.D.OR.200 din Anexa nr. 2 la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;

6.6. după punctul ATM/ANS.AR.C.025 se completează cu punctul ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Modificări ale sistemului de management al securității informațiilor**

(a) Pentru modificările gestionate și notificate AAC în conformitate cu procedura prevăzută la subpct. 13.1. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, AAC include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. ATM/ANS.AR.C.010. În cazul în care se constată o neconformitate, AAC notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. ATM/ANS.AR.C.050.

(b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu subpct. 13.2. IS.I.OR.255 din Anexa nr. 2 (partea IS.I.OR) la Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației:

1. la primirea cererii de efectuare a modificării, AAC verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;

2. AAC stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării;

3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”

6.7. La Anexa nr. 3 CERINȚE PENTRU FURNIZORII DE ATM/ANS (partea ATM/ANS.OR), după punctul ATM/ANS.OR.B.005 se completează cu punctul ATM/ANS.OR.B.005A:

„ATM/ANS.OR.B.005A Sistemul de management al securității informațiilor

Pe lângă sistemul de management menționat la pct. ATM/ANS.OR.B.005, furnizorul de servicii instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul privind cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;

6.8. punctul ATM/ANS.OR.D.010 se modifică:

„ **ATM/ANS.OR.D.010 Managementul securității**

(a) Furnizorii de servicii de navigație aeriană și de management al fluxului de trafic aerian și administratorul rețelei, ca parte integrantă a sistemului lor de management, astfel cum se prevede la pct. ATM/ ANS.OR.B.005, trebuie să instituie un sistem de management al securității pentru a asigura:

1. securitatea facilităților și a personalului lor, în vederea prevenirii actelor de intervenție ilicită în furnizarea serviciilor;

2. securitatea datelor operaționale pe care le primesc, le produc sau le utilizează în alt mod, astfel încât accesul la acestea să fie rezervat exclusiv persoanelor autorizate.

(b) Sistemul de management al securității trebuie să definească:

1. procesele și procedurile referitoare la evaluarea și reducerea riscurilor de securitate, monitorizarea și îmbunătățirea securității, examinările de securitate și diseminarea rezultatelor;

2. mijloacele destinate să identifice, să monitorizeze și să detecteze breșele de securitate și să alerteze personalul prin semnale de avertizare adecvate cu privire la securitate;

3. mijloacele de control al efectelor cauzate de breșele de securitate și de identificare a măsurilor de remediere și a procedurilor de reducere a riscurilor pentru prevenirea repetării acestora.

(c) Furnizorii de servicii de navigație aeriană și de management al fluxului de trafic aerian și administratorul rețelei trebuie să asigure autorizarea de securitate a personalului propriu, dacă este cazul, și să se coordoneze cu autoritățile civile și militare relevante pentru a asigura securitatea facilităților, a personalului și a datelor lor.

(d) Aspectele legate de securitatea informațiilor trebuie gestionate în conformitate cu pct. ATM/ ANS.OR.B.005A.”