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.”

NOTĂ DE FUNDAMENTARE
la proiectul hotărârii Guvernului 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

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul hotărârii Guvernului 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 a fost elaborat de către Ministerul Infrastructurii și Dezvoltării Regionale *(MIDR)* în comun cu Autoritatea Aeronautică Civilă *(AAC).*

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Proiectul hotărârii Guvernului 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 este elaborat în ***scopul*** armonizării cadrului normativ național cu standardele Uniunii Europene, obligativitatea racordării cadrului normativ național cu acquis-ul comunitar pe domeniul aviației civile conform Anexei III al Acordului privind spațiul aerian comun între Uniunea Europeană şi statele sale membre şi Republica Moldova (*în continuare ASAC*), semnat la Bruxelles la data de 26.06.2012, ratificat prin Legea nr. 292/2012.

Necesitatea transpunerii acestuia derivă din prevederile Anexei III la ASAC, Capitolul C „Siguranța Aeronautică" și Programul Național de Aderare a Republicii Moldova la UE (PNA) 2025-2029, aprobat prin Hotărârea de Guvern nr. 306/2025, CLUSTER 4. AGENDA VERDE ȘI CONECTIVITATE SUSTENABILĂ, Capitolul 14 „POLITICA DE TRANSPORT", „Transport aerian", Anexa A, acțiunea nr. 200 și nr. 210.

Scopul prezentului proiect este ***transpunerea totală*** a prevederilor următoarelor Regulamente:

1. 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.

2. 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.

În sensul prezentului Regulament, ***se aplică prevederile*** din Codul aerian al Republicii Moldova nr. 301/2017, precum și prevederi din următoarele Regulamente, care sunt prevăzute ajustarea lor conform noilor prevederi reglementate în prezentul proiect de act normativ:

- 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, adoptat prin Hotărârea de Guvern nr. 91/2024;
- Regulamentul privind procedurile administrative referitoare la aerodromuri, adoptat prin Hotărârea de Guvern nr. 653/2018;
- Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, adoptat prin Hotărârea de Guvern nr. 119/2023;
- Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, adoptat prin Hotărârea de Guvern nr. 134/2019;
- Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, adoptat prin Hotărârea de Guvern nr. 204/2020;
- Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, adoptat prin Hotărârea de Guvern nr. 612/2022.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Semnarea la Bruxelles la 26 iunie 2012 a ASAC, Republica Moldova și-a asumat obligația de a ajusta cadrul normativ național în domeniul aviației civile la cel european prin implementarea actelor normative europene stabilite în Anexa III. Acest lucru a devenit și mai important în contextul în care Republica Moldova a devenit stat candidat pentru aderarea la UE, statut confirmat de către Consiliul European la 23 iunie 2022.

În acest sens, pentru realizarea obligației statutului asumat prin ASAC, este necesară transpunerea în cadrul normativ național a Regulamentului delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022 și a Regulamentului de punere în aplicare (UE) 2023/203 al Comisiei din 27 octombrie 2022., privind securitatea informațiilor cu impact potențial asupra siguranței aviației.

Riscurile în materie de securitate a informațiilor sunt în continuă creștere în domeniul aviației civile, pe măsură ce sistemele informatice actuale devin tot mai interconectate și devin tot mai des ținta unor terți răuintenționați. Respectivele riscuri în materie de securitate pot proveni din diverse surse, cum ar fi deficiențe de proiectare și de întreținere, aspecte ale performanțelor umane, amenințări la adresa mediului și amenințări la adresa securității informațiilor.

Prin urmare, sistemele de management instituite de autoritățile naționale competente responsabile de supravegherea industriei aeronautice și de organizațiile menționate, în considerentele expuse, trebuie să țină seama nu doar de riscurile în materie de siguranță care decurg din evenimente inopinate, ci și de riscurile în materie de siguranță care decurg din amenințări la adresa securității informațiilor, atunci când deficiențele existente pot fi exploatate de persoane cu intenții răuvoitoare. Riscurile asociate acestor sisteme informatice nu se limitează la posibile atacuri asupra spațiului cibernetic, ci includ și amenințări care pot afecta procesele și procedurile, precum și performanțele ființelor umane.

La nivel internațional, un număr semnificativ de organizații utilizează deja standarde internaționale, cum ar fi ISO 27001, pentru a aborda securitatea informațiilor și a datelor digitale. Aceste standarde pot să nu abordeze pe deplin specificul aviației civile, respectiv, este necesară instituirea unor cerințe specifice privind managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.

Scopul acestor cerințe este ca să se acopere toate domeniile aviației civile și interfețele acestora, dat fiind că aviația este un sistem de sisteme cu grad înalt de interconectare.

Obiectivul de bază îl constituie instituirea și menținerea unui sistem de management pentru gestionarea riscurilor în materie de securitate a informațiilor de către:

- organizațiile de management al continuității navigabilității;
- organizațiile de întreținere;
- organizațiile de pregătire a piloților,;
- organizațiile de pregătire a echipajului de cabină;
- centrele de medicină aeronautică pentru personalul aeronautic navigant;
- și operatorii de echipamente de pregătire sintetică pentru zbor;
- operatorii aerieni;
- furnizorii de servicii de management al traficului aerian;
- furnizorii de servicii de navigație aeriană;
- furnizorii de servicii U-spac și furnizorii unici de servicii de informații;
- organizațiile de pregătire și centrele de medicină aeronautică pentru controlorii de trafic aerian;
- organizațiilor aprobate implicate în proiectarea sau producția de sisteme ATM/ANS.

Temei special pentru prezentul proiect de hotărâre a Guvernului cu privire la aprobarea proiectului servesc dispozițiile art. 76 din Legea nr. 100/2017 care stabilesc reexaminarea în vederea actualizării actelor normative, pentru evaluarea compatibilității cu alte acte normative în vigoare la momentul reexaminării, precum și cu reglementările legislației UE, în conformitate cu angajamentele internaționale ale Republicii Moldova.

Regulamentul vine cu ***propuneri de soluționare a unor probleme prioritare pentru Republica Moldova***, precum:

- Instituirea unui sistem național de management al riscurilor de securitate cibernetică în aviație, pentru creșterea nivelului securității cibernetice și protecția infrastructurii critice aeronautice, asigurând continuitatea operațiunilor în siguranță;
- instruirea și specializarea personalului din autoritatea de reglementare și supraveghere în domeniul aeronautic și securității informațiilor, cu privire la creșterea eficienței și profesionalismului structurilor de control și monitorizare;
- modernizarea infrastructurii aeroportuare prin aplicarea tehnologiilor digitale pentru gestionarea fluxurilor și pentru managementul riscurilor, în scopul creșterii siguranței, eficienței și operativității aeronautice.

În concluzie**:** Regulamentul prevede cerințe referitoare la managementul riscurilor în materie de securitate a informațiilor, pentru gestionarea riscurilor legate de securitatea informațiilor în domeniul aviației, pentru protejarea infrastructurii, datelor și a sistemelor electronice critice.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul național are ca ***obiectiv principal*** transpunerea a două Regulamente comunitare:

1. Regulamentul delegat (UE) 2022/1645, în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor prevede cerințele către organizații pentru identificarea și gestionarea riscurilor legate de securitatea informațiilor, care pot afecta siguranța aviatică.

Aceste riscuri pot influența sistemele tehnologice informaționale, datele utilizate în aviația civilă. **Scopul** este de a identifica evenimentele de securitate a informațiilor, de a identifica incidentele ce pot avea impact asupra siguranței aviatice și de a asigura răspunsul și recuperarea corespunzătoare în urma acestora. Aspectele cheie prevăzute sunt:

- **Stabilirea unui sistem de management al securității informațiilor.** Operatorii și autoritățile 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; implementarea și menținerea unui sistem eficient de identificare, evaluare și management al riscurilor asociate securității informațiilor, pentru a preveni amenințările cibernetice și alte vulnerabilități;
- **Stabilirea procedurilor pentru identificarea, raportarea, evaluarea și tratarea riscurilor.** Este necesar efectuarea analizei periodice pentru identificarea amenințărilor și vulnerabilităților relevante în sistemele informatice și de comunicație utilizate în domeniu;
- **Implementarea unor măsuri de securitate** pe baza evaluărilor de risc, elaborarea măsurilor tehnice și organizaționale pentru protejarea informațiilor sensibile, pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor;
- **Elaborarea Planurilor de răspuns la incidente.** Este imperativ să existe planuri și proceduri clar definite pentru gestionarea incidentelor de securitate a informațiilor, pentru a limita impactul și a preveni răspândirea acestora;
- **Elaborarea Manualului de management al securității informațiilor,** constituie elaborarea unui document comprehensiv (MMSI) care descrie politicile, responsabilitățile, resursele și procedurile pentru gestionarea riscurilor de securitate a informațiilor, conform cerințelor legislației, și menține actualitatea acestuia prin actualizări regulate și aprobări, asigurând o gestionare sistematică și eficientă a securității informațiilor, protejând sistemele și datele critice, prevenind incidentele de securitate și garantând conformitatea cu cerințele legale și de siguranță;
- **Cerințele și competențele în formarea personalului** implicat trebuie să fie instruit periodic în privința riscurilor de securitate a informațiilor și a măsurilor de protecție;
- **Monitorizarea și auditul politicilor de securitate,** prevede elaborarea și menținerea unui sistem de evidențe pentru toate activitățile legate de managementul securității informațiilor, inclusiv aprobări, evaluări de risc, contracte, incidente, vulnerabilități, calificări ale personalului și evenimente. Astfel, asigurând trasabilitatea, responsabilitatea și controlul asupra tuturor activităților și deciziilor legate de securitatea informațiilor, facilitând auditul, reevaluările și gestionarea riscurilor, precum și protejarea integrității și confidențialității evidențelor.

2. Regulamentul de punere în aplicare (UE) 2023/203 de stabilire a normelor de aplicare a în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, stabilește norme pentru gestionarea riscurilor legate de securitatea informațiilor cu impact asupra siguranței aviației. Prevede următoarele cerințe pentru organizații și autorități din domeniul aviației, pentru a asigura o abordare sistematică în evaluarea și controlul riscurilor legate de securitatea informațiilor, în conformitate cu multiplele reglementări UE din domeniu și în scopul îmbunătățirii gestionării riscurilor în siguranța aviației, precum:

- **Identificarea 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;
- **Detectarea evenimentelor de securitate a informațiilor** și a identificării celor care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației;

➢ **Asigurarea unui răspuns la respectivele incidente de securitate** a informațiilor și a redresării în urma acestora.

Totodată, Regulamentul prevede că organizațiile trebuie să păstreze evidențe detaliate și trasabile ale activităților legate de managementul securității informațiilor, inclusiv aprobări, evaluări de risc, contracte, incidente, vulnerabilități și evenimente, pentru o perioadă minimă de cinci ani. De asemenea, trebuie să păstreze evidențele personalului implicat și să asigure protecția și integritatea acestor evidențe, conform procedurilor interne și nivelului de clasificare.

Prin ***prevederile actului normativ*** se urmărește:

- instituirea normelor generale privind obiectivul și domeniul de aplicare;
- definirea noțiunilor specifici obiectului de reglementare;
- stabilirea instituțiilor naționale responsabile de implementarea reglementărilor.

Proiectul include trei anexe:

➢ ***Anexa nr. 1*** - stabilește cerințe în materie de management care trebuie îndeplinite de AAC în calitate de organ responsabil de activități de certificare, de supraveghere și de asigurare a respectării conformității. Respectiv, instituie necesitatea creării în cadrul AAC a unui sistem de management al securității informațiilor în cadrul căruia vor fi evaluate riscurile în materie de securitate a informațiilor, tratarea acestora, precum și detectarea/răspunsul și redresarea incidentelor de securitate a informațiilor, atât în cadrul instituției cât și identificate în cadrul supravegherii organizațiilor;

➢ ***Anexa nr. 2*** - stabilește cerințele care trebuie îndeplinite de organizațiile din domeniul aviației civile precum organizațiilor de producție și organizațiilor de proiectare, organizațiilor de întreținere, organizațiilor de management al continuității navigabilității, operatorilor de aerodromuri și furnizorilor de servicii de gestionare a platformei, operatorilor aerieni, organizațiilor de pregătire aprobate (ATO-uri), centrelor de medicină aeronautică pentru personalul navigant, operatorilor de echipamente de pregătire sintetică pentru zbor (FSTD-uri), organizațiilor de pregătire a controlorilor de trafic aerian (ATCO) și centrele de medicină aeronautică pentru ATCO, furnizorii de servicii de navigație aeriană care dețin un certificat limitat, furnizorilor de servicii de informare a zborurilor etc.

➢ ***Anexa nr. 3 –*** stabilește modificarea a șase Regulamente care vor fi suspuse unor modificări corespunzătoare prin completarea acestora cu prevederi ce se referă la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, precum:

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, adoptat prin Hotărârea de Guvern nr. 91/2024;
2. Regulamentului privind procedurile administrative referitoare la aerodromuri, adoptat prin Hotărârea de Guvern nr. 653/2018;
3. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, adoptat prin Hotărârea de Guvern nr. 204/2020;
4. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, adoptat prin Hotărârea de Guvern nr. 612/2022;
5. Regulamentul de stabilire a cerințelor și procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, adoptat prin Hotărârea de Guvern nr. 134/2019;
6. Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, adoptat prin Hotărârea de Guvern nr. 119/2023.

Prevederile proiectului sunt incluse și în proiectul Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea

organizațiilor şi a personalului cu atribuţii în domeniu; inclusiv celor care au deja obligația de a dispune de un sistem de management în conformitate cu standardele internaționale în domeniul siguranței aviației, proiect definitivat, remis la promovare.

Rezultatele scontate după adoptarea și implementarea prezentului proiect de act normativ, se urmărește asigurarea punerii în aplicare consecventă în toate domeniile aviației, și implementarea de toate organizațiile (inclusiv de AAC) care cad sub incidența prezentului Regulament, fiind important la alinierea proceselor/mecanismelor în materie de securitate cibernetică în domeniul aviației civile naționale la cele internaționale, pentru a asigura coerența și compatibilitatea între acestea. Acest proces este deosebit de important în domeniul aviației civile, deoarece aviația este o industrie globală, iar operarea în mod sigur și eficient necesită standarde comune și reglementări uniforme.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În cadrul normativ național nu este transpus actualmente un șir de regulamente europene precum Regulamentul delegat (UE) 2022/1645 și Regulamentul de punere în aplicare (UE) 2023/203.

Acest proces a devenit și mai important în contextul în care Republica Moldova a devenit stat-candidat pentru aderarea la UE. Astfel, procesul de transpunere a acquis-lui european, inclusiv în domeniul aviației civile, trebuie să fie unul cât se poate mai aproape și cât se poate mai rapid posibil.

În acest sens, pentru realizarea obligației statutului asumat prin ASAC, sunt necesare transpunerea în cadrul normativ național a Regulamentelor enunțate.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Impactul asupra sectorului public este determinat de următoarele aspecte:

1. **Obligațiunile în elaborarea și implementarea cerințelor de management al riscurilor în domeniul securității aviației** – autoritățile și organismele publice conformarea cu privire la corelarea și implementarea măsurilor mai stricte pentru asigurarea securității informațiilor.

2. **Necesitatea de conformare și monitorizare** – sectorul public va trebui să adapteze cadrul legislativ, operațional și de control pentru a respecta noile norme, implicând creșterea eforturilor de conformare și inspecții și auditări pentru a se asigura că acestea aplică măsurile de management al riscurilor conform Regulamentului.

3. **Costuri suplimentare pentru implementare** – pentru autoritățile de reglementare și de inspecție, pot apărea costuri legate de instruirea personalului, actualizarea sistemelor și procedurilor, precum și supravegherea continuă.

4. **Îmbunătățirea gestionării riscurilor** – responsabilizarea autorităților pentru gestionarea riscurilor în securitatea informațiilor, ceea ce, pe termen lung, contribuie la siguranța generală a sectorului aeronautic.

5. **Coordonare mai strânsă între autorități și organizații** – la nivelul statelor membre, cooperarea și schimbul de informații se vor intensifica pentru a asigura conformitatea și pentru a răspunde mai eficient la riscurile emergente.

În concluzie, Regulamentul aduce un impact semnificativ, dar optim pentru sectorul public, solicitând alocarea de resurse suplimentare și adaptarea proceselor pentru a asigura o gestionare eficientă

a riscurilor tehnologice și de securitate în domeniul aviației civile, contribuind la siguranța sectorului aeronautic.

4.2. Impactul financiar și argumentarea costurilor estimative

Impactul financiar cu privire la implementarea cerințelor prevăzute în prezentul Regulament implică costuri pentru următoarele acțiuni:

- Necesitatea de a dezvolta sau ajusta sisteme și proceduri interne pentru gestionarea riscurilor;
- Costurile cu formarea personalului sau cu consultanță specializată;
- Investiții în tehnologie sau echipamente pentru monitorizarea și controlul riscurilor;
- Costuri administrative pentru conformitate și audituri.

Astfel, pentru organizații se impune alocarea surselor financiare precum:

- **Costurile tehnologice,** investiții în sistemele informatice pentru stocarea, protejarea și gestionarea evidențelor digitale. Costuri pentru implementarea sau actualizarea platformelor de management al securității și de raportare;
- **Costurile pentru personal**. Angajarea sau instruirea personalului specializat în gestionarea, monitorizarea și asigurarea protecției și păstrării evidențelor împotriva deteriorării, alterării sau furtului, conform noilor cerințe.
- **Costurile de conformare și audit,** pentru auditurile periodice pentru verificarea respectării cerințelor de păstrare a evidențelor precum și pentru elaborarea și menținerea documentației și procedurilor interne conform noilor reguli.
- **Costurile administrative și de training** pentru personalul implicat în managementul securității și păstrarea evidențelor. Actualizarea politicilor și procedurilor interne în conformitate cu noile reglementări.
- **Costurile legate de riscuri și incidente:** Creșterea nivelului de securitate pentru a evita pierderea, deteriorarea sau compromiterea evidențelor, care ar putea avea consecințe financiare semnificative. Asigurarea unor procese eficiente pentru identificarea, raportarea și tratarea incidentelor de securitate, pentru a evita costurile legate de incidentele de securitate.
- **Costuri legate de securitatea fizică și digitală:** Investiții în măsuri de protecție a datelor, inclusiv criptare, control acces de date sigure, menținerea unor medii de stocare sigure, conforme cu nivelurile de clasificare a informațiilor.

În concluzie**:** Alocarea resurselor financiare atât pentru conformare, cât și pentru menținerea sistemelor și personalului necesar, poate duce la creșteri considerabile ale costurilor operaționale. Totuși, aceste investiții conduc la un nivel mai ridicat de securitate și responsabilitate, reducând riscurile de incidente costisitoare și asigurând conformitatea cu reglementările europene.

Astfel, la implementarea prezentului proiect de act normativ pot fi necesare cheltuieli financiare din bugetul de stat.

Notă: Pentru elucidarea și analiza impactului financiar prin scrisoarea MIDR nr. 13-2812 din 26 mai 2025 a fost solicitată din partea instituțiilor /companiilor vizate opinia asupra impactului financiar, direct sau indirect asupra procesului instituțional, cheltuieli, investițiile necesare, perioada de tranziție, date statistice, alte propuneri vizavi de aspectele financiare, în contextul implementării și conformării normelor europene, în scopul îmbunătățirii siguranței aviației civile. La etapa de preavizare propuneri și obiecții nu au fost expuse. Menționăm că, la etapa de avizare proiectul va fi remis în mod repetat către industria aeronautică.

1.3. Impactul asupra sectorului privat

Impactul asupra sectorului privat este cauzat de modul în care companiile din domeniul aviației și al serviciilor conexe gestionează securitatea informațiilor, iar principalele efecte pot fi următoarele:

1. **Creșterea responsabilităților și a obligațiilor de conformare.** Companiile trebuie să implementeze sau să își actualizeze sistemele de management al riscurilor de securitate a informațiilor pentru a respecta noile cerințe, fiind necesară documentarea proceselor, evaluarea constantă a riscurilor și adoptarea de măsuri preventive și corective.
2. **Costuri pentru implementare și întreținere**. Investiții în tehnologiile de securitate, infrastructură IT și formarea personalului pentru a asigura conformitatea, costuri legate de audituri periodice, teste de vulnerabilitate și actualizarea continuă a măsurilor de securitate.
3. **Necesitatea formării personalului și instruirii pe segmentul managementul riscurilor de securitate**. Angajații trebuie instruiți pentru a identifica și gestiona riscurile de securitate și pentru a răspunde adecvat incidentelor de securitate a informațiilor, în crearea unei culturi organizaționale orientate spre securitate.
4. **Îmbunătățirea securității operaționale și de informații**. Investițiile și finanțarea au drept scop final asigurarea unei securități sporite, pentru reducerea riscului de atacuri cibernetice, vulnerabilități și alte incidente care pot avea efecte financiare și reputaționale grave, dar și a fi un pericol la securitatea operațională a companiei. Totodată, va determina creșterea încrederii pasagerilor în sistemele și serviciile oferite.
5. **Necesitatea cooperării și schimbului de informații.** Companiile aeriene trebuie să colaboreze mai strâns cu autoritățile și alte organizații pentru schimbul de informații despre riscuri și incidente, creând rețele de securitate mai robuste.

În concluzie, sectorul privat va trebui să aloce resurse pentru implementarea și menținerea unui nivel ridicat de securitate a informațiilor, să devină mai responsabili în gestionarea riscurilor, și să își reconfigureze procesele pentru a respecta noile norme, în siguranța proceselor operaționale și a pasagerilor cu scop final asigurarea unei securități sporite, pentru reducerea riscului de atacuri cibernetice, vulnerabilități și alte incidente.

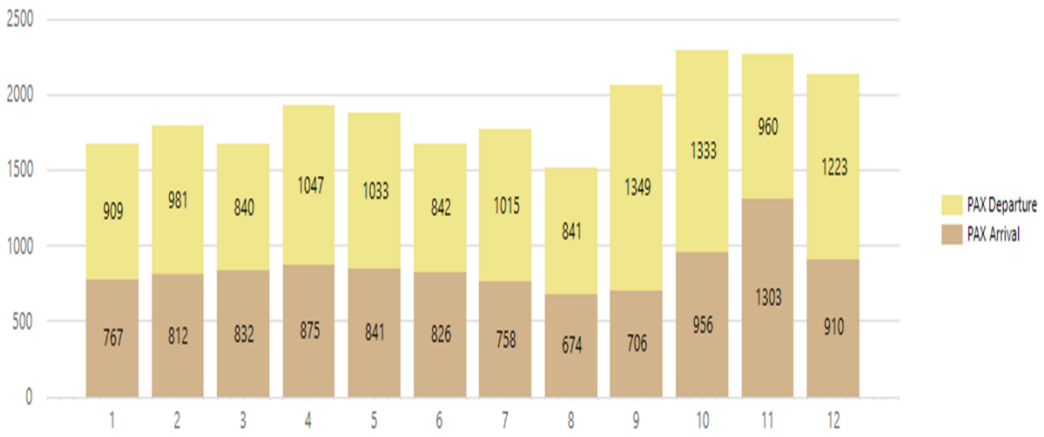
4.4. Impactul social

Contribuția în acest sector se definește prin necesitatea dezvoltării unei securități robuste în spațiul aerian care să ofere nivelul necesar de siguranță, de capacitate, de reacție, de coordonare, de performanță de mediu și de furnizare continuă a serviciilor aeriene rapide, ținând seama în mod corespunzător de necesitățile de securitate și apărare.

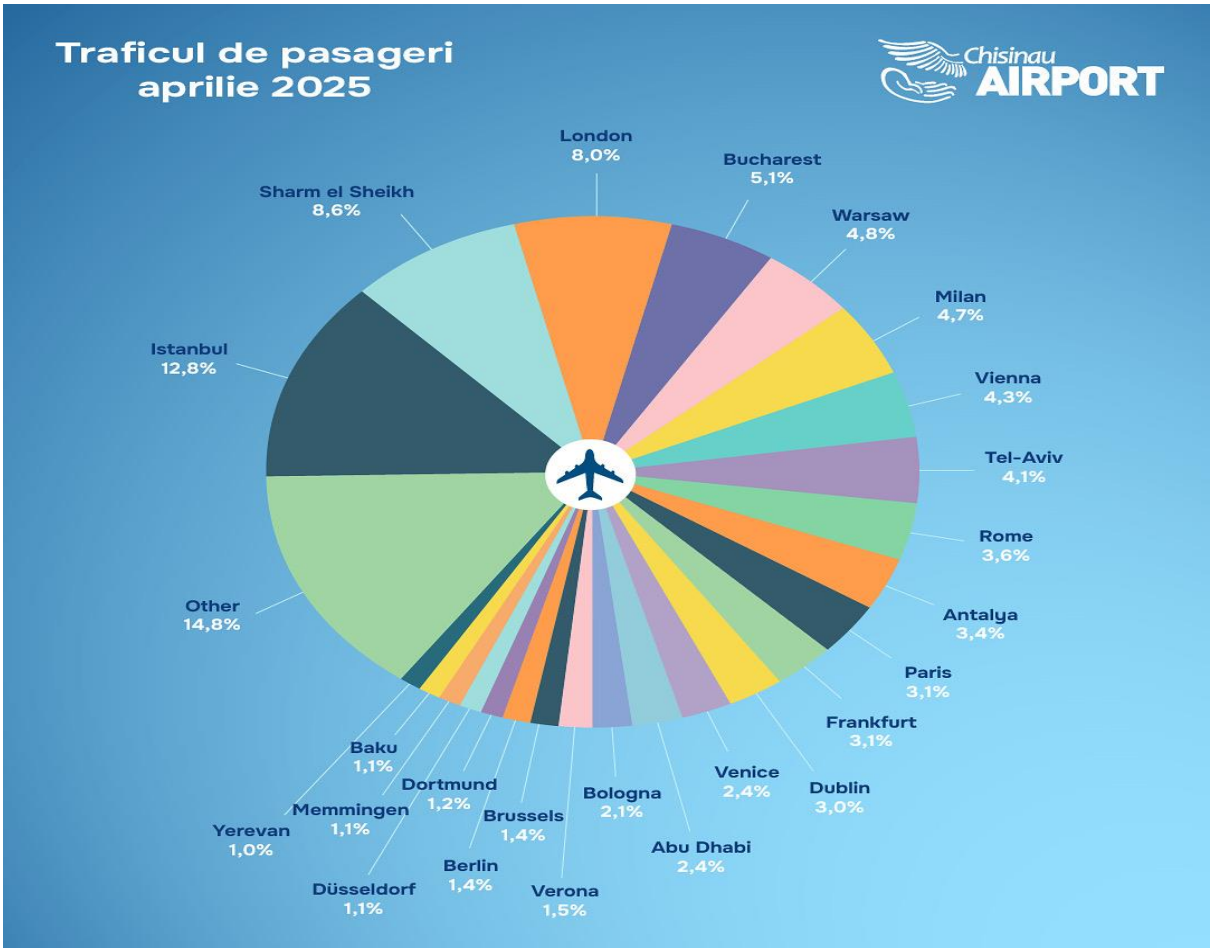
Pe măsura creșterii numărului de pasageri (*se anexează graficele fluxului de pasageri per oră pentru perioada anilor 2023 - 2024)* și pentru a face față cererii tot mai mare a cetățenilor, contribuția în acest sector se definește prin importanța securității informațiilor și a gestionării riscurilor în domeniul aviației, ceea ce poate duce la o mai mare înțelegere și încredere în sistemul de transport aerian, asigurând menținerea unui nivel ridicat de siguranță al aviației, dar și măsuri echilibrate pentru mediul social.

Graficele fluxului de pasageri per oră pentru perioada 2024/2025

Summer 2024 (31.03.2024-02.11.2024) Maximum PAX per hour (UTC)



Aeroportul Internațional Chișinău a încheiat luna aprilie 2025 cu un trafic total de 388.122 pasageri îmbarcați și debarcați, reprezentând 155,2% realizare față de prognoza estimată. Comparativ cu aceeași perioadă a anului 2024, se constată o creștere de 60%, echivalentul a +145.617 pasageri. În aceeași perioadă, pe segmentul cargo au fost înregistrate 190,4 tone de mărfuri.



Astfel, impactul social, este de durată, cu caracter pozitiv, care poate fi evaluat pe viitor în baza indicatorilor de monitorizare raportați la riscul de incidente sau atacuri asupra infrastructurii aeronautice, ceea ce sporește siguranța pasagerilor și al publicului larg, eficiența și operativitatea în coordonare între entități.

Totodată, măsurile de securitate mai stricte pot implica proceduri de control mai riguroase, ceea ce poate influența confortul și libertățile individuale, dar acestea sunt justificate în numele siguranței colective.

În concluzie, impactul social al acestui proiect este determinat pe de o parte, de creșterea încrederii în siguranța transporturilor aeriene și responsabilizarea societății în gestionarea riscurilor, iar pe de altă parte, pot apărea preocupări legate de intimitate și libertăți personale, în special în contextul măsurilor stricte de securitate, proces în final, indispensabil, cu scopul asigurării siguranței traficului aerian.

4.4.1. Impactul asupra datelor cu caracter personal

În procesul de implementare și executare a proiectului de act normativ prelucrarea datelor cu caracter personal se va face strict prin asigurarea protecției drepturilor şi libertăților fundamentale ale persoanei fizice cu privire la prelucrarea datelor cu caracter personal conform Legii nr. 133/2011 privind protecția datelor cu caracter personal.

În unele cazuri, măsurile de securitate avansate și monitorizarea riscurilor pot fi percepute de anumite segmente ale societății ca o formă de supraveghere excesivă, ceea ce poate genera dezbateri legate de intimitate și libertăți civile, dar procedurile efectuate se vor face strict conform cadrului normativ în scopul asigurării securității și siguranței aeronautice.

4.4.2. Impactul asupra echității și egalității de gen

Prezentul Regulament nu are impact asupra echității și egalității de gen.

4.5. Impactul asupra mediului

Aplicarea unor principii de performanță și utilizarea de tehnologii inovatoare este esențială pentru îmbunătățirea continuă a proceselor operaționale pe domeniul transportului aerian, determinând o mai bună gestionare a riscurilor de securitate ce pot preveni incidente majore, inclusiv cele care pot avea consecințe grave asupra mediului, precum pierderea unui avion sau accidente care pot duce la deversări de combustibil sau alte substanțe periculoase.

Astfel, *impactul direct asupra mediului* este mai puțin evident decât în alte domenii, gestionarea riscurilor și implementarea tehnologiilor avansate pot avea, pe termen lung, efecte favorabile prin prevenirea accidentelor, promovarea practicilor mai durabile și stimularea sectorului să adopte soluții sustenabile în procesele operaționale.

4.6. Alte impacturi și informații relevante

Posibile impacturi pot fi identificate asupra competitivității sectorului, fiind determinat de rapiditatea și conformarea la noile cerințe a organizațiilor.

De asemenea, poate fi sesizat impactul asupra inovației tehnologice, determinată de necesitatea de a satisface cerințele de securitate și gestionarea riscurilor pentru stimularea, dezvoltarea și adoptarea de noile tehnologii și soluții inovatoare, inclusiv inteligență artificială, tehnologii de analiză a datelor pentru prevenirea incidentelor.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Proiectul național transpune prevederile:

- **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; și

- **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.

Prezentele Regulamente stabilesc cerințele pentru implementarea și menținerea unor măsuri adecvate pentru protejarea informațiilor și asigurarea siguranței aeronautice, gestionarea riscurilor legate de securitatea informațiilor și a securității aviației, cooperarea între autorități și organizații pentru schimbul de informații de securitate, pregătirea și conștientizarea personalului implicat în gestionarea riscurilor și securitatea informațiilor, fiind expuse următoarele elemente:

a) obiectivele actului juridic al UE:

REGULAMENTUL DELEGAT (UE) 2022/1645 AL COMISIEI din 14 iulie 2022 prevede cerințele care trebuie îndeplinite de organizațiile din sectorul aviației în vederea 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, în vederea detectării evenimentelor de securitate a informațiilor și a identificării acelora care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației, precum și în vederea asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) nr. 2023/203 AL COMISIEI din 27 octombrie 2022, stabilește cerințele pe care trebuie să le îndeplinească organizațiile și autoritățile competente în vederea:

- 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;

- detectării evenimentelor de securitate a informațiilor și a identificării celor care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației;
- asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.

b) gradul de transpunere a actului juridic al UE, precizându-se dacă transpunerea este totală, parțială sau selectivă:

Proiectul național transpune total prevederile Regulamentului de punere în aplicare (UE) 2023/203 al Comisiei din 27 octombrie 2022 și a Regulamentului delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022.

c) argumentarea introducerii unor reglementări care nu sunt prevăzute expres în actul juridic al UE şi/sau care depășesc cerințele minime stabilite de acesta:

Proiectul de act normativ și Tabelele de concordanță sunt elaborate potrivit rigorilor Legii nr. 100/2017 cu privire la actele normative și Hotărârea Guvernului nr. 1171/2018 pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene.

Proiectul hotărârii va fi supus expertizei de compatibilitate cu legislația UE, conform art. 35 din Legea nr. 100/2017 cu privire la actele normative.

Informația privind rezultatele expertizei de compatibilitate cu legislația UE urmează a fi inclusă în sinteza obiecțiilor și propunerilor/recomandărilor urmare recepționării raportului din partea Centrului de Armonizare a Legislației.

Din punct de vedere al compatibilității prevederile UE sunt compatibile în raport cu prevederile actului juridic național.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Prezentul Regulament este elaborat în baza Regulamentului delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022 și a Regulamentului delegat (UE) 2022/1645 al Comisiei din 14 iulie 2022.

Necesitatea transpunerii acestuia derivă din prevederile Anexei III la ASAC, Capitolul C „Siguranța Aeronautică” și Programul Național de Aderare a Republicii Moldova la UE (PNA) 2025-2029, aprobat prin Hotărârea de Guvern nr. 306/2025, CLUSTER 4., AGENDA VERDE ȘI CONECTIVITATE SUSTENABILĂ, Capitolul 14. „POLITICA DE TRANSPORT”, „Transport aerian”, Anexa A, acțiunea nr. 200 și nr. 210.

În concluzie, menționăm necesitatea executării obligațiilor Republicii Moldova conform Convenției privind aviația civilă internațională și ASAC în mod uniform în toate țările UE și în Republica Moldova, fiind atinse obiectivele Convenției privind aviația civilă internațională și a Acordului privind spațiul aerian comun dintre Republica Moldova şi Uniunea Europeană şi statele sale membre.

6. Avizarea și consultarea publică a proiectului actului normativ

În scopul respectării prevederilor Legii nr.239/2008 privind transparența în procesul decizional, anunțul cu privire la inițierea elaborării proiectului a fost plasat pe pagina web oficială a Ministerului Infrastructurii și Dezvoltării Regionale (compartimentul „Transparența", directoriul „Transparență decizională/Anunțuri de inițiere a politicilor"), și pe portalul guvernamental particip.gov.md, la data de 24.02.2025, la adresa - https://particip.gov.md/ro/document/stages/*/14009.

A fost solicitată către industria aeronautică consultarea prealabilă a proiectului prin scrisoarea MIDR nr. 13-2812 din 26 mai 2025.

Proiectul urmează a fi consultat și avizat cu instituțiile publice de resort în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative, inclusiv:

- Ministerul Dezvoltării Economice și Digitalizării (inclusiv Agenția pentru Securitatea Cibernetică), Ministerul Apărării, Ministerul Finanțelor, Ministerul Afacerilor Interne, Ministerul Afacerilor Externe, Serviciul de Informații și Securitate, Agenția Proprietății Publice, Consiliul Concurenței, Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației, Biroul de Investigare a Accidentelor și Incidentelor în Transporturi, Autoritatea Aeronautică Civilă;
- Î.S. "MoldATSA";
- Î.S. „Aeroportul Internațional Chișinău";
- Î.S. „Aeroportul Internațional Mărculești";
- Operatorii aerieni.

Informația privind rezultatele avizării va fi inclusă în sinteză după recepționarea avizelor respective.

7. Concluziile expertizelor

Proiectul va fi supus prezentării către autoritățile publice responsabile pentru efectuarea expertizei de compatibilitate cu legislația UE și ulterior expertizei anticorupție și a expertizei juridice, conform art. 34 din Legea nr.100/2017 cu privire la actele normative. Concluziile expertizelor vor fi incluse în nota de fundamentare la proiectul actului normativ. Astfel, în cadrul procesului de elaborare a proiectului sunt incluse următoarele constatări:

a) Constatările expertizei de compatibilitate

Proiectul va fi supus expertizei de compatibilitate cu legislația UE în conformitate cu prevederile art. 35 din Legea nr. 100/2017 cu privire la actele normative, fiind prezentată expertiza Centrului de Armonizare a Legislației. Urmare recepționării expertizei de compatibilitate cu legislația UE, Tabelul de compatibilitate va fi ajustat, iar concluziile vor fi reflectate în Sinteza proiectului.

b) Constatările expertizei anticorupție

Proiectul va fi remis spre expertizare Centrului Național Anticorupție în conformitate cu prevederile art. 36 din Legea nr. 100/2017 cu privire la actele normative.

Informația privind rezultatele expertizei anticorupție urmează a fi inclusă în sinteza obiecțiilor și propunerilor/recomandărilor urmare recepționării Raportului anticorupție.

c) Constatările expertizei juridice

Proiectul va fi remis spre expertizare Ministerului Justiției conform art. 37 din Legea nr.100/2017 cu privire la actele normative.

Informația privind rezultatele expertizei juridice urmează a fi inclusă în sinteza obiecțiilor și propunerilor/recomandărilor urmare recepționării Raportului de expertiză juridică.

8. Modul de încorporare a actului în cadrul normativ existent

Prezentul proiect de hotărâre stabilește modificarea Regulamentelor care vor fi suspuse unor modificări corespunzătoare prin completarea acestora cu prevederi ce se referă la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, precum:

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, adoptat prin Hotărârea de Guvern nr. 91/2024;

2. Regulamentului privind procedurile administrative referitoare la aerodromuri, adoptat prin Hotărârea de Guvern nr. 653/2018;

3. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, adoptat prin Hotărârea de Guvern nr. 204/2020;

4. Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, adoptat prin Hotărârea de Guvern nr. 612/2022;

5. Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, adoptat prin Hotărârea de Guvern nr. 134/2019;

6. Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, adoptat prin Hotărârea de Guvern nr. 119/2023.

7. Regulamentul privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu; inclusiv celor care au deja obligația de a dispune de un sistem de management în conformitate cu standardele internaționale în domeniul siguranței aviației, proiect în proces de promovare.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

În scopul implementării cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației prezentul Regulament se aplică următoarelor părți implicate sau entităților care acționează în numele acestora:

1) Autoritatea Aeronautică Civilă, în ceea ce privește supravegherea organizațiilor care pun în aplicare cerințele de management al securității informațiilor;
2) utilizatorii spațiului aerian al Republicii Moldova;
3) furnizorul de servicii de navigație aeriană din Republica Moldova;
4) administratorilor de aeroporturi din Republica Moldova.

Totodată, proiectul prevede pentru autoritățile și organizațiile din sectorul aerian responsabilitatea de a dezvolta și implementa măsuri de securitate și de management al riscurilor, prin identificarea, gestionarea, evaluarea și controlul riscurilor de securitate a informațiilor, formarea personalului și respectarea confidențialității datelor, colaborarea internațională și schimbul de informații. implementarea de măsuri pentru protecția datelor și gestionarea activităților legate de securitatea informațiilor.

În concluzie, menționăm că prin proiectul de hotărâre a Guvernului 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 se propune soluții ce vizează întărirea sectorului aeronautic, asigurând conformitatea cu reglementările europene, modernizarea infrastructurii, creșterea securității și a eficienței. Implementarea lor va consolida poziția Republicii Moldovei în domeniu și va stimula dezvoltarea durabilă a industriei aeronautice naționale.

Secretar general **Angela ȚURCANU**

Ministerul Infrastructurii
și Dezvoltării Regionale
al Republicii Moldova

Nr. 13 – 3155 din 12.06.2025

Cancelaria de Stat

Prin prezenta, în conformitate cu pct.197 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr.610/2018, remitem pentru înregistrare proiectul hotărârii Guvernului ***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 lista proiectelor, care urmează a fi examinate în cadrul următoarei ședințe a Secretarilor generali.

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	**Criterii de înregistrare**	**Nota autorului**
1.	Categoria și denumirea proiectului	Proiect de hotărâre de Guvern 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.
2.	Autoritatea care a elaborat proiectul	Ministerul Infrastructurii și Dezvoltării Regionale de comun cu Autoritatea Aeronautică Civilă.
3.	Justificarea depunerii cererii *(indicația corespunzătoare sau remarca precum că proiectul este elaborat din inițiativa autorului)*	Proiectul are drept scop transpunerea prevederilor: - *Regulamentului 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;

		- *Regulamentului 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. *Obiectivul* prezentului Regulament îl constituie instituirea și menținerea unui sistem de management pentru gestionarea riscurilor în materie de securitate a informațiilor în domeniul aviației, pentru protejarea infrastructurii, datelor și a sistemelor electronice critice. Proiectul de hotărâre stabilește și modificarea Regulamentelor care vor fi suspuse unor modificări corespunzătoare prin completarea acestora cu prevederi ce se referă la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, menționate în Nota de fundamentare.
3[1].	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte documente de planificare sectoriale)*	- Programul Național de Aderare a Republicii Moldova la UE (PNA) 2025- 2029, CLUSTER 4., AGENDA VERDE ȘI CONECTIVITATE SUSTENABILĂ, Capitolul 14. „POLITICA DE TRANSPORT”, „Transport aerian”, Anexa A., acțiunea nr.200 și nr.210, aprobat prin Hotărârea Guvernului nr. 306/2025; - Prevederile Anexei III a Acordului privind spațiul aerian comun între Uniunea Europeană şi statele sale membre şi Republica Moldova, semnat la Bruxelles, pe 26.06.2012, ratificat prin Legea nr. 292/2012, Capitolul C „Siguranța Aeronautică”.
4.	Lista autorităților și instituțiilor a căror avizare este necesară	*Avizare:* 1. Ministerul Dezvoltării Economice și Digitalizării *(inclusiv Agenția pentru Securitatea Cibernetică și*

		Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației); 2. Ministerul Apărării; 3. Ministerul Finanțelor; 4. Ministerul Afacerilor Interne; 5. Ministerul Afacerilor Externe; 6. Serviciul de Informații și Securitate; 7. Agenția Proprietății Publice (*inclusiv, Î.S. "MoldATSA", Î.S. „Aeroportul Internațional Chișinău", Î.S. „Aeroportul Internațional Mărculești")*; 8. Consiliul Concurenței; 9. Biroul de Investigare a Accidentelor și Incidentelor în Transporturi. *Expertizare:* Centrul de Armonizare a Legislației.
5.	Termenul-limită pentru depunerea avizelor/expertizelor	10 zile lucrătoare.
6.	Persoana responsabilă de promovarea proiectului	Tatiana BUDU – Consultant principal, Serviciul politici în domeniul transportului aerian. Tel. 022 250-549 E-mail: tatiana.budu@midr.gov.md
7.	Anexe	1. Proiectul hotărârii de Guvern -52 file; 2. Nota de fundamentare -14 file; 3. Tabelul de concordanță R (UE) 2023/203 -139 file; 4. Tabelul de concordanță R (UE) 2022/1645 - 46 file; 5. Sinteza – 4 file.
8.	Data și ora depunerii cererii	
9.	Semnătura	

Secretar general **Angela ȚURCANU**

SINTEZA
la proiectul Hotărârii Guvernului 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

Nr.	Participantul la avizare (expertizare)/consultare publică, expertizare	Conținutul obiecției/ Propunerii, recomandării, concluziei	Se acceptă/ Nu se acceptă	Argumentarea autorului proiectului
Avizare și consultare publică *(prealabilă)*				
1.	**Î.S. „Aeroportul Internațional Chișinău, scrisoarea nr.03/936 din 12.06.2025**	*Lipsă sugestii și obiecții.* În partea ce tine de impactul financiar pentru conformare și perioada de implementare, comunicam că Regulamentul impune explicit implementarea unui sistem de management al securității informațiilor *(în continuare - SMSI)* bazat pe analiza riscurilor, documentarea și revizuirea continuă a proceselor și controalelor, instruirea personalului și stabilește un set de cerințe pentru implementare a SMSI în cadrul I.S. ‚AIC" cum ar fi: ***1.*** achiziția sistemelor pentru managementul securității informațiilor (SIEM, soluții de detecție a incidentelor, platforme de raportare și analiză, sisteme de audiții monitorizare rețea). ***2.*** modernizarea infrastructurii hardware (servere dedicate, echipamente de backup și redundanță). ***3.*** implementarea și actualizarea software-ului pentru controlul accesului, criptare, gestiunea vulnerabilităților, managementul evenimentelor de securitate.	**Se ia act**	

		4. elaborarea și actualizarea politicilor interne de management al riscurilor. ***5.*** documentarea procedurilor, rolurilor responsabilităților, păstrarea evidențelor, cel puțin 5 ani. ***6.*** implementarea auditului intern, pregătirea rapoartelor periodice către autorități. ***7.*** integrarea cu sistemele de raportare/supraveghere a Autorității Aeronautice Civile și Agenția pentru Securitatea Cibernetică. ***8.*** instruirea periodică a personalului privind cerințele procedurile, simulări de incidente, instruire pe platforme noi. ***9.*** certificarea personalului responsabil cu managementul informațiilor. ***10.*** sesiuni de conștientizare pentru angajați, testări periodice. ***11.*** actualizări regulate de software, licențe, contracte de suport. ***12.*** audituri externe pentru validarea conformității. ***13.*** mentenanță și operare a sistemelor, evaluării upgrade-uri periodice etc. Ținând cont de cele relatate, Î.S. ,AIC" urmare a unei analize detaliate a impactului financiar asociat acestei inițiative va planifica pentru anul 2026 cheltuielile și costurile aferente implementării Regulamentului.		

Tabel de Concordanță

1. Titlul actului Uniunii Europene 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
2. Titlul proiectului de act normative național Proiectul hotărârii Guvernului cu privire la aprobarea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației, și de modificare a unor hotărâri ale Guvernului
3. Gradul de compatibilitate Compatibil
4. Autoritatea/persoana responsabilă Ministerul Infrastructurii și Dezvoltării Regionale, de comun cu Autoritatea Aeronautică Civilă
5. Data întocmirii/actualizării Mai 2025

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Articolul 1 Obiect În prezentul regulament sunt prevăzute cerințele pe care trebuie să le îndeplinească organizațiile și autoritățile competente în vederea: (a) 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; (b) detectării evenimentelor de securitate a informațiilor și a identificării celor care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației; (c) asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.	**PHG** **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.	Compatibil	Lipsă
Articolul 2 Domeniu de aplicare (1) Prezentul regulament se aplică următoarelor organizații: (a) organizații de întreținere supuse dispozițiilor din secțiunea A din anexa II (partea 145) la Regulamentul (UE) nr. 1321/2014, cu excepția celor implicate exclusiv	**2.** Prezentul Regulament se aplică următoarelor organizații: 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	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
în întreținerea aeronavelor în conformitate cu anexa Vb (partea ML) la Regulamentul (UE) nr. 1321/2014;	în domeniu, cu excepția celor implicate exclusiv în întreținerea aeronavelor în conformitate cu anexa nr. 5b (partea ML);		domeniu, și de abrogare a unei Hotărâri
(b) organizații de management al continuității navigabilității (CAMO-uri) supuse dispozițiilor din secțiunea A din anexa Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014, cu excepția celor implicate exclusiv în managementul continuității navigabilității aeronavelor în conformitate cu anexa Vb (partea ML) la Regulamentul (UE) nr. 1321/2014;	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 și a personalului cu atribuţii în domeniu, cu excepția celor implicate exclusiv în managementul continuității navigabilității aeronavelor în conformitate cu anexa nr. 5b (partea ML);	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(c) operatori aerieni supuși dispozițiilor din anexa III (partea ORO) la Regulamentul (UE) nr. 965/2012, cu excepția celor implicați exclusiv în operarea oricăreia dintre următoarele: (i) o aeronavă ELA 2, astfel cum este definită la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012; (ii) avioane monomotoare cu elice cu o configurație maximă operațională de cinci locuri pentru pasageri sau mai puțin, care nu sunt clasificate drept aeronave complexe	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, adoptat 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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; (iii) 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;	producţie, adoptat 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;		
(d) organizații de pregătire aprobate (ATO-uri) supuse dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011, cu excepția celor implicate exclusiv în activități de pregătire aferente aeronavelor ELA 2, astfel cum sunt definite la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012, sau implicate exclusiv în pregătire teoretică;	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, adoptat prin HG 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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, adoptat prin Hotărârea de Guvern nr. 91/2024, sau implicate exclusiv în pregătire teoretică;		
(e) centre de medicină aeronautică pentru personalul navigant supuse dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011;	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, adoptat prin Hotărârea de Guvern nr. 204/2020;	Compatibil	Lipsă
(f) operatori de echipamente de pregătire sintetică pentru zbor (FSTD-uri) supuși dispozițiilor din anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011, cu excepția celor implicați exclusiv în operarea FSTD-urilor aferente aeronavelor ELA 2, astfel cum sunt definite la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012;	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, adoptat 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	produselor, pieselor şi echipamentelor aferente, precum şi cerinţele referitoare la capacitatea organizaţiilor de proiectare şi producţie, adoptat prin Hotărârea de Guvern nr. 91/2024;		
(g) organizații de pregătire a controlorilor de trafic aerian (ATCO) și centre de medicină aeronautică pentru ATCO supuse dispozițiilor din anexa III (partea ATCO.OR) la Regulamentul (UE) 2015/340;	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, adoptat prin Hotărârea de Guvern nr. 134/2019;	Compatibil	Lipsă
(h) organizații supuse dispozițiilor din anexa III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373, cu excepția următorilor furnizori de servicii: (i) furnizori de servicii de navigație aeriană care dețin un certificat limitat în conformitate cu punctul ATM/ ANS.OR.A.010 din anexa menționată; (ii) furnizori de servicii de informare a zborurilor care își declară activitățile în conformitate cu punctul ATM/ ANS.OR.A.015 din anexa menționată;	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, adoptat 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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(i) furnizori de servicii U-space și furnizori unici de servicii de informații comune care sunt supuși dispozițiilor din Regulamentul de punere în aplicare (UE) 2021/664;	2.11. furnizorilor de servicii U-space și furnizorilor unici de servicii de informații;	Compatibil	Lipsă
(j) organizații aprobate implicate în proiectarea sau producția de sisteme ATM/ANS și de componente ATM/ANS care fac obiectul Regulamentului de punere în aplicare (UE) 2023/1769 al Comisiei (1).	2.12. organizațiilor aprobate implicate în proiectarea sau producția de sisteme ATM/ANS și de componente ATM/ANS;		
(2) Prezentul regulament se aplică autorităților competente, inclusiv Agenției Uniunii Europene pentru Siguranța Aviației („agenția”), astfel cum sunt menționate la articolul 6 din prezentul regulament și la articolul 5 din Regulamentul delegat (UE) 2022/1645 al Comisiei (2).	**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”)*.	Compatibil	Lipsă
(3) Prezentul regulament se aplică, de asemenea, autorității competente responsabile cu eliberarea, prelungirea, modificarea, suspendarea sau revocarea licențelor de întreținere a aeronavelor în conformitate cu anexa III (partea 66) la Regulamentul (UE) nr. 1321/2014.	**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”)*.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(4) Prezentul regulament nu aduce atingere cerințelor privind securitatea informațiilor și securitatea cibernetică stabilite la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 și la articolul 14 din Directiva (UE) 2016/1148.	**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.	Compatibil	Lipsă
Articolul 3 Definiții În sensul prezentului regulament, se aplică următoarele definiții: 1. „securitate a informațiilor” înseamnă păstrarea confidențialității, integrității, autenticității și disponibilității rețelelor și sistemelor informatice; 2. „eveniment de securitate a informațiilor” înseamnă 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. „incident” înseamnă orice eveniment care are un efect negativ real asupra securității rețelelor și	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
sistemelor informatice, astfel cum este definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148; 4. „risc în materie de securitate a informațiilor” înseamnă riscul la adresa organizării operațiunilor de aviație civilă, precum și la adresa activelor, a persoanelor fizice și a altor organizații, atribuibil 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; 5. „amenințare” înseamnă o încălcare potențială a securității informațiilor care există atunci când o entitate, o circumstanță, o acțiune sau un eveniment ar putea cauza prejudicii; 6. „vulnerabilitate” înseamnă 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.	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Articolul 4 Cerințe pentru organizații și pentru autorități competente (1) Organizațiile menționate la articolul 2 alineatul (1) trebuie să respecte cerințele din anexa II (partea IS.I.OR) la prezentul regulament.	**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.	Compatibil	Lipsă
(2) Autoritățile competente menționate la articolul 2 alineatele (2) și (3) trebuie să respecte cerințele din anexa I (partea IS.AR) la prezentul regulament.	**9.** Cerințele aplicabile AAC sunt stabilite în anexa nr. 1 [PARTEA IS.AR], la prezentul Regulament.	Compatibil	Lipsă
Articolul 5 Cerințe care decurg din alte acte legislative ale Uniunii (1) Atunci când o organizație menționată la articolul 2 alineatul (1) îndeplinește cerințe de securitate stabilite în conformitate cu articolul 14 din Directiva (UE) 2016/1148 care sunt echivalente cu cerințele stabilite în prezentul regulament, se consideră că îndeplinirea respectivelor cerințe de securitate constituie îndeplinirea cerințelor stabilite în prezentul regulament.	-	Norme UE neaplicabile	Prevederi tranzitorii în contextul în care Directiva (UE) 2016/1148 a fost abrogată.
(2) În cazul în care o organizație menționată la articolul 2 alineatul (1) este un operator sau o entitate menționată în programele naționale	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
de securitate a aviației civile ale statelor membre, stabilite în conformitate cu articolul 10 din Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului (3), cerințele de securitate cibernetică de la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 trebuie considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.I.OR.230 din anexa II la prezentul regulament, care trebuie respectat ca atare.	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.		
(3) În cazul în care organizația menționată la articolul 2 alineatul (1) este furnizorul de servicii de navigație aeriană al Serviciului european geostaționar mixt de navigare (EGNOS) menționat în Regulamentul (UE) 2021/696, cerințele de securitate prevăzute în titlul V articolele 33-43 din regulamentul respectiv sunt considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.I.OR.230 din anexa II la prezentul regulament, care trebuie respectat ca atare.	-	Norme UE neaplicabile	furnizorul de servicii de navigație aeriană național nu reprezintă Serviciul european geostaționar mixt de navigare (EGNOS)
(4) După consultarea agenției și a grupului de cooperare menționat la articolul 11 din Directiva (UE)	-	Norme UE neaplicabile	Prevederi exclusiv destinate SM

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2016/1148, Comisia poate să emită orientări pentru evaluarea echivalenței cerințelor stabilite în prezentul regulament și în Directiva (UE) 2016/1148.			
Articolul 6 Autoritatea competentă (1) Fără a aduce atingere sarcinilor încredințate consiliului de acreditare de securitate menționat la articolul 36 din Regulamentul (UE) 2021/696, autoritatea responsabilă cu certificarea și supravegherea respectării prezentului regulament este: (a) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (a), autoritatea competentă desemnată în conformitate cu anexa II (partea 145) la Regulamentul (UE) nr. 1321/2014;	**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”).*	Compatibil	Lipsă
(b) în ceea ce privește organizațiile menționate la articolul 2 litera (b), autoritatea competentă desemnată în conformitate cu anexa III (partea ADR.OR) la Regulamentul (UE) nr. 139/2014.	**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”).*	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (c), autoritatea competentă desemnată în conformitate cu anexa III (partea ORO) la Regulamentul (UE) nr. 965/2012;	**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”)*.	Compatibil	Lipsă
(d) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) literele (d)-(f), autoritatea competentă desemnată în conformitate cu anexa VII (partea ORA) la Regulamentul (UE) nr. 1178/2011;	**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”)*.	Compatibil	Lipsă
(e) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (g), autoritatea competentă desemnată în conformitate cu articolul 6 alineatul (2) din Regulamentul (UE) 2015/340;	**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”)*.	Compatibil	Lipsă
(f) în ceea ce privește organizațiile menționate la articolul 2 alineatul	**4.** Autoritatea responsabilă de supravegherea şi controlul respectării	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(1) litera (h), autoritatea competentă desemnată în conformitate cu articolul 4 alineatul (1) din Regulamentul de punere în aplicare (UE) 2017/373;	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”)*.		
(g) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (i), autoritatea competentă desemnată în conformitate cu articolul 14 alineatul (1) sau cu articolul 14 alineatul (2) din Regulamentul de punere în aplicare (UE) 2021/664, după caz;	**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”)*.	Compatibil	Lipsă
(h) în ceea ce privește organizațiile menționate la articolul 2 alineatul (1) litera (j), autoritatea competentă desemnată în conformitate cu articolul 3 alineatul (1) din Regulamentul de punere în aplicare (UE) 2023/1769.	**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”)*.	Compatibil	Lipsă
(2) În sensul prezentului regulament, statele membre pot desemna o entitate independentă și autonomă care să îndeplinească rolul și responsabilitățile atribuite	**5.** AAC, în vederea realizării supravegherii şi controlul respectării prevederilor prezentului Regulament, antrenează în activitatea sa autoritatea competentă la nivel naţional în domeniul	Parțial compatibil	La nivel național a fost creată prin HG nr. 1028/2023 Agenția pentru Securitatea Cibernetică

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
autorităților competente menționate la alineatul (1). În acest caz, trebuie stabilite măsuri de coordonare între entitatea respectivă și autoritățile competente, astfel cum se menționează la alineatul (1), pentru a se asigura supravegherea efectivă a tuturor cerințelor care trebuie respectate de către organizație.	securității cibernetice - *Agenția pentru Securitatea Cibernetică (în continuare „ASC”)*, în conformitate cu prevederile Regulamentului cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, adoptat prin Hotărârea de Guvern nr. 1028/2023 și altor acte conexe. **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.		
(3) Agenția cooperează, în deplină conformitate cu normele aplicabile privind confidențialitatea, protecția datelor cu caracter personal și protecția informațiilor clasificate, cu Agenția Uniunii Europene pentru Programul spațial (EUSPA) și cu consiliul de acreditare de securitate menționat la articolul 36 din Regulamentul (UE) 2021/696, pentru a asigura supravegherea eficace a cerințelor aplicabile furnizorului de servicii de navigație aeriană al EGNOS.	**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.	Parțial Compatibil	Prevederi UE neaplicabile destinare instituțiilor Europene
Articolul 7 Transmiterea informațiilor relevante către autoritățile competente din domeniul NIS	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Autoritățile competente în temeiul prezentului regulament comunică, fără întârzieri nejustificate, punctului unic de contact desemnat în conformitate cu articolul 8 din Directiva (UE) 2016/1148 orice informație relevantă inclusă în notificările transmise în temeiul punctului IS.I.OR.230 din anexa II la prezentul regulament și în temeiul punctului IS.D.OR.230 din anexa I la Regulamentul delegat (UE) 2022/1645 de către operatorii de servicii esențiale identificați în conformitate cu articolul 5 din Directiva (UE) 2016/1148. Modificări aduse Regulamentului (UE) nr. 748/2012	Cibernetică, adoptat 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.		
Articolul 8 Modificarea Regulamentului (UE) nr. 1178/2011 Anexele VI (partea ARA) și VII (partea ORA) la Regulamentul (UE) nr. 1178/2011 se modifică în conformitate cu anexa III la prezentul regulament.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*	Compatibil	Lipsă
Articolul 9 Modificarea Regulamentului (UE) nr. 748/2012	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor*	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Anexa I (partea 21) la Regulamentul (UE) nr. 748/2012 se modifică în conformitate cu anexa IV la prezentul regulament.	*referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*		
Articolul 10 Modificarea Regulamentului (UE) nr. 965/2012 Anexele II (partea ARO) și III (partea ORO) la Regulamentul (UE) nr. 965/2012 se modifică în conformitate cu anexa V la prezentul regulament.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*	Compatibil	Lipsă
Articolul 11 Modificarea Regulamentului (UE) nr. 139/2014 Anexa II (partea ADR.AR) la Regulamentul (UE) nr. 139/2014 se modifică în conformitate cu anexa VI la prezentul regulament.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*	Compatibil	Lipsă
Articolul 12 Modificarea Regulamentului (UE) nr. 1321/2014 Anexele II (partea 145), III (partea 66) și Vc (partea CAMO) la	PHG cu privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Regulamentul (UE) nr. 1321/2014 se modifică în conformitate cu anexa VII la prezentul regulament.	de abrogare a unei Hotărâri în proces de promovare (pe platforma Guvernamentală)		
Articolul 13 Modificarea Regulamentului (UE) 2015/340 Anexele II (partea ATCO.AR) și III (partea ATCO.OR) la Regulamentul (UE) 2015/340 se modifică în conformitate cu anexa VIII la prezentul regulament.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*	Compatibil	Lipsă
Articolul 14 Modificarea Regulamentului de punere în aplicare (UE) 2017/373 Anexele II (partea ATM/ANS.AR) și III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373 se modifică în conformitate cu anexa IX la prezentul regulament.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației*	Compatibil	Lipsă
Articolul 15 Modificarea Regulamentului de punere în aplicare (UE) 2021/664 1. La articolul 15 alineatul (1), litera (f) se înlocuiește cu următorul text: „(f) implementează și menține un sistem de management al securității în conformitate cu punctul ATM/	Actul UE va fi transpus în sem. II 2025	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
ANS.OR.D.010 din subpartea D a anexei III la Regulamentul de punere în aplicare (UE) 2017/373 și un sistem de management al securității informațiilor în conformitate cu anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.” 2. La articolul 18 se adaugă următoarea literă (l): „(l) instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203.”			
Articolul 16 Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene. Se aplică de la 22 februarie 2026. În cazul furnizorului de servicii de navigație aeriană al EGNOS, care se supune dispozițiilor Regulamentului de punere în aplicare (UE) 2017/373, prezentul regulament se aplică însă de la 1 ianuarie 2026.	**Hotărârea de Guvern**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.			
ANEXĂ **SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE AUTORITĂȚILOR** **[PARTEA IS.AR]**			
IS.AR.100 Domeniul de aplicare Prezenta parte stabilește cerințele în materie de management care trebuie îndeplinite de organizațiile menționate la articolul 2 alineatul (2) din prezentul regulament. Cerințele pe care trebuie să le îndeplinească autoritățile competente respective când își desfășoară activitățile de certificare, de supraveghere și de asigurare a respectării sunt cuprinse în regulamentele menționate la articolul 2 alineatul (1) din prezentul regulament și la articolul 2 din Regulamentul delegat (UE) 2022/1645.	**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. .	Compatibil	Lipsă
IS.AR.200 Sistemul de management al securității informațiilor (SMSI) (a) Pentru a atinge obiectivele prevăzute la articolul 1, autoritatea	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
competentă trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că autoritatea competentă: 1. instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale autorității competente în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației; 2. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.AR.205; 3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.AR.210; 4. definește și implementează, în conformitate cu punctul 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	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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
respectivele incidente de securitate a informațiilor și se redresează în urma acestora; 5. îndeplinește cerințele de la punctul IS.AR.220 când subcontractează altor organizații orice parte a activităților descrise la punctul IS.AR.200; 6. îndeplinește cerințele în materie de personal de la punctul IS.AR.225; 7. îndeplinește cerințele de păstrare a evidențelor de la punctul IS.AR.230; 8. monitorizează îndeplinirea de către propria organizație a cerințelor din prezentul regulament și transmite persoanei menționate la punctul IS.AR.225 litera (a) feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective; 9. protejează confidențialitatea oricăror informații pe care autoritatea competentă le-ar putea avea cu privire la organizații care fac obiectul supravegherii sale și a informațiilor primite prin	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
intermediul sistemelor de raportare externă ale organizației, instituite în conformitate cu punctul IS.I.OR.230 din anexa II (partea IS.I.OR) la prezentul regulament și cu punctul IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645; 10. notifică agenției schimbările care afectează capacitatea autorității competente de a-și executa sarcinile și de a-și îndeplini responsabilitățile definite în prezentul regulament; 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 alte autorități și agenții competente, precum și organizațiile supuse dispozițiilor prezentului regulament să efectueze evaluări eficace ale riscurilor în materie de securitate asociate activităților lor.			
(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1, autoritatea competentă trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.AR.235.	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) Autoritatea competentă trebuie să documenteze toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.AR.200 litera (a) și să instituie un proces de modificare a acestei documentații.	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.	Compatibil	Lipsă
(d) Procesele, procedurile, rolurile și responsabilitățile instituite de autoritatea competentă pentru a se conforma punctului IS.AR.200 litera (a) 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 autoritatea competentă.	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.	Compatibil	Lipsă
IS.AR.205 Evaluarea riscurilor în materie de securitate a informațiilor (a) Autoritatea competentă trebuie să identifice toate elementele propriei organizații care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea cuprind:	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. activitățile, instalațiile și resursele autorității competente și serviciile pe care le operează, furnizează, primește sau menține autoritatea competentă; 2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor menționate la subpunctul 1.	funcționarea elementelor menționate la subpct. 3.1.1.		
(b) Autoritatea competentă trebuie să identifice interfețele pe care propria organizație le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.	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.	Compatibil	Lipsă
(c) Pentru elementele și interfețele menționate la literele (a) și (b), autoritatea competentă trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, autoritatea competentă trebuie: 1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de autoritatea competentă; 2. să asocieze fiecare risc și nivelul său aferent cu elementul sau	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
interfața corespunzătoare identificată în conformitate cu literele (a) și (b). Clasificarea predefinită menționată la subpunctul 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 autorității competente, a unui proces structurat și repetabil de management al riscurilor pentru operațiuni, autoritatea competentă trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu punctul IS.AR.210. Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în conformitate cu subpunctul 1 se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).	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.		
(d) Autoritatea competentă trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și (c) în oricare dintre următoarele cazuri:	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:	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor; 2. când există o modificare a interfețelor dintre autoritatea competentă și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații; 3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor; 4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.	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.		
IS.AR.210 Tratarea riscurilor în materie de securitate a informațiilor (a) Autoritatea competentă trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.AR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită autorității competente: 1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;	**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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. să diminueze consecințele pentru siguranța aviației care sunt asociate materializării scenariului de amenințare; 3. să evite riscurile. Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.	Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.		
(b) Persoana menționată la punctul IS.AR.225 litera (a) și ceilalți membri vizați ai personalului autorității competente trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul IS.AR.205, de scenariile de amenințare corespunzătoare și de măsurile care trebuie implementate. Autoritatea competentă trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu punctul IS.AR.205 litera (b) cu privire la orice risc comun autorității competente și organizației în cauză.	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.	Compatibil	Lipsă
IS.AR.215 Incidentele de securitate a informațiilor – detectare, răspuns și redresare	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.AR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul IS.AR.210, autoritatea competentă 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 autorității competente: 1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale; 2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.	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.		
(b) Autoritatea competentă trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Respectivele măsuri de răspuns trebuie să permită autorității competente:	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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. să declanșeze reacția propriei organizații la avertizările menționate la litera (a) subpunctul 2 prin activarea unor resurse și planuri de acțiune predefinite; 2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare; 3. să controleze modul de defectare al elementelor afectate definite la punctul IS.AR.205 litera (a).	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.		
(c) Autoritatea competentă 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 autorității competente: 1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil; 2. să restabilească starea de siguranță a elementelor afectate definite la punctul IS.AR.205 litera (a) în timpul de redresare definit în prealabil de propria organizație.	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
IS.AR.220 Subcontractarea activităților de management al securității informațiilor Autoritatea competentă trebuie să se asigure, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul IS.AR.200, că activitățile subcontractate respectă cerințele din prezentul regulament și că organizația subcontractată lucrează sub supravegherea sa. Autoritatea competentă trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.	**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.	Compatibil	Lipsă
IS.AR.225 Cerințele în materie de personal Autoritatea competentă trebuie: (a) 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. 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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. să aibă drepturile statutare pentru accesarea deplină a resurselor necesare pentru ca autoritatea competentă să îndeplinească toate sarcinile prevăzute în prezentul regulament; 2. să dețină delegarea de competențe necesară pentru îndeplinirea atribuțiilor primite;	7.1.2. să dețină delegarea de competențe necesară pentru îndeplinirea atribuțiilor primite;		
(b) să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru desfășurarea activităților reglementate de prezenta anexă;	7.2. să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru desfășurarea activităților reglementate de prezenta Anexă;	Compatibil	Lipsă
(c) să dispună de o procedură prin care să se asigure că personalul menționat la litera (b) are competența necesară pentru a-și îndeplini sarcinile;	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;	Compatibil	Lipsă
(d) să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite;	7.4. să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite;	Compatibil	Lipsă
(e) 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.	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.	Compatibil	Lipsă
IS.AR.230 Păstrarea evidențelor	**IS.AR.230 Păstrarea evidențelor**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) Autoritatea competentă trebuie să păstreze evidența activităților sale de management al securității informațiilor. 1. Autoritatea competentă trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile: (i) contractele pentru activitățile menționate la punctul IS.AR.200 litera (a) subpunctul 5; (ii) evidențele proceselor-cheie menționate la punctul IS.AR.200 litera (d); (iii) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.AR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.AR.210; (iv) 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. 2. Evidențele menționate la subpunctul 1 punctul (i) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
3. Evidențele menționate la subpunctul 1 punctele (ii) și (iii) se păstrează timp de cel puțin cinci ani. 4. Evidențele menționate la subpunctul 1 punctul (iv) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de autoritatea competentă.			
(b) Autoritatea competentă trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor. 1. Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru autoritatea competentă și timp de cel puțin trei ani după ce persoana a părăsit autoritatea competentă. 2. Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, autoritatea competentă trebuie să le furnizeze acestora, la părăsirea	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
autorității competente, o copie a evidențelor personale.			
(c) Formatul evidențelor se specifică în procedurile autorității competente.	8.3. Formatul evidențelor se specifică în procedurile AAC.	Compatibil	Lipsă
(d) 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. Autoritatea competentă trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.	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.		
IS.AR.235 Îmbunătățirea continuă (a) Autoritatea competentă 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 autoritatea competentă, sau în urma unui incident de securitate a informațiilor.	**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.	Compatibil	Lipsă
(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) se constată deficiențe, autoritatea competentă trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
respecte cerințele aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, autoritatea competentă trebuie să reevalueze elementele SMSI-ului vizate de măsurile adoptate.	materie de securitate a informațiilor la un nivel acceptabil. În plus, AAC trebuie să reevalueze elementele SMSI-ului vizate de măsurile adoptate.		
ANEXA II **SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE ORGANIZAȚIILOR** **[PARTEA IS.I.OR]**			
IS.I.OR.100 Domeniul de aplicare Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la articolul 2 alineatul (1) din prezentul regulament.	**Anexa nr. 2** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* **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.	Compatibil	Lipsă
IS.I.OR.200 Sistemul de management al securității informațiilor (SMSI)	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) Pentru a atinge obiectivele prevăzute la articolul 1, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația: 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. identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.205; 3. definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.210; 4. implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu punctul IS.I.OR.215;	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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
5. definește și implementează, în conformitate cu punctul 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 punctului IS.I.OR.205 litera (e), asigură un răspuns la respectivele incidentele de securitate a informațiilor și se redresează în urma acestora; 6. implementează măsurile care au fost notificate de autoritatea competentă ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației; 7. ia măsurile corespunzătoare, în conformitate cu punctul IS.I.OR.225, pentru abordarea constatărilor notificate de autoritatea competentă; 8. implementează un sistem de raportare externă în conformitate cu punctul IS.I.OR.230, astfel încât autoritatea competentă să poată lua măsuri corespunzătoare;	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
9. îndeplinește cerințele de la punctul IS.I.OR.235 când subcontractează altor organizații orice parte a activităților menționate la punctul IS.I.OR.200; 10. îndeplinește cerințele în materie de personal stabilite la punctul IS.I.OR.240; 11. îndeplinește cerințele de păstrare a evidențelor stabilite la punctul IS.I.OR.245; 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; 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.	funcție de nivelul de sensibilitate a informațiilor respective.		
(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1,	2.2. Pentru a îndeplini în permanență cerințele menționate la subpct. 2.1.1.,	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.I.OR.260.	organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu pct. 14. IS.I.OR.260.		
(c) Organizația trebuie să documenteze, în conformitate cu punctul IS.I.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.I.OR.200 litera (a) și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu punctul IS.I.OR.255.	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.	Compatibil	Lipsă
(d) Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma punctului IS.I.OR.200 litera (a) 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.	2.4. 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.	Compatibil	Lipsă
(e) Fără a se aduce atingere obligației de conformitate cu cerințele de raportare stabilite în	2.5. Fără a se aduce atingere obligației de conformitate cu cerințele de raportare stabilite în reglementarea aeronautică	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Regulamentul (UE) nr. 376/2014 și cu cerințele stabilite la punctul IS.I.OR.200 litera (a) subpunctul 13, organizația poate primi din partea autorității competente aprobarea de a nu implementa cerințele menționate la literele (a)-(d) și cerințele aferente de la punctele IS.I.OR.205-IS.I.OR.260 dacă demonstrează într-un mod considerat satisfăcător de autoritatea respectivă 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 punctul IS.I.OR.205 și examinată și aprobată de autoritatea sa competentă. Menținerea valabilității respectivei aprobări va fi examinată de autoritatea competentă în urma ciclului de audit de supraveghere	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.			
IS.I.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor (a) Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă: 1. activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația; 2. echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpunctul 1.	**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.	Compatibil	Lipsă
(b) 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.	3.2. 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.	Compatibil	Lipsă
(c) În ceea ce privește elementele și interfețele menționate la literele (a) și (b), organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie: 1. să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație; 2. să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu literele (a) și (b). Clasificarea predefinită menționată la subpunctul 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 punctul IS.I.OR.210. Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
temeiul subpunctului 1 se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).			
(d) Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și, după caz, (c) sau (e) în oricare dintre următoarele situații: 1. când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor; 2. când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații; 3. când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor; 4. când analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.	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.	Compatibil	Lipsă
(e) Prin derogare de la litera (c), organizațiile care trebuie să respecte subpartea C din anexa III (partea ATM/ANS.OR) la Regulamentul de	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
punere în aplicare (UE) 2017/373 înlocuiesc analiza impactului asupra siguranței aviației cu o analiză a impactului asupra serviciilor lor, în conformitate cu evaluarea în sprijinul siguranței prevăzută la punctul 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.	stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, adoptat 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.		
IS.I.OR.210 Tratarea riscurilor în materie de securitate a informațiilor (a) Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.I.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației:	**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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare; 2. să diminueze consecințele asupra siguranței aviației care sunt asociate materializării scenariului de amenințare; 3. să evite riscurile. Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.	Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.		
(b) Persoana menționată la punctul IS.I.OR.240 literele (a) și (b) și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul 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 punctul IS.I.OR.205 litera (b) cu privire la orice risc comun celor două organizații.	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.	Compatibil	Lipsă
IS.I.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor	**5. IS.I.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) 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 punctului IS.I.OR.230.	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.		
(b) Sistemul respectiv și procesul menționat la punctul IS.I.OR.220 trebuie să permită organizației: 1. să identifice care dintre evenimentele raportate în temeiul literei (a) sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației; 2. să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul 1 și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu punctele IS.I.OR.205 și IS.I.OR.220; 3. să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a	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.;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul 1; 4. să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.	5.2.4. să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.		
(c) 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 litera (b).	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.	Compatibil	Lipsă
(d) Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.	5.4. Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.	Compatibil	Lipsă
(e) Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.	5.5. Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.	Compatibil	Lipsă
IS.I.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare	**6. IS.I.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.I.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul 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: 1. să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale; 2. să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.	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.		
(b) Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) 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. 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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. să declanșeze reacția la avertizările menționate la litera (a) subpunctul 2 prin activarea unor resurse și planuri de acțiune predefinite; 2. să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare; 3. să controleze modul de defectare al elementelor afectate definite la punctul IS.I.OR.205 litera (a).	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.		
(c) 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: 1. să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil; 2. să asigure atingerea unei stări de siguranță a elementelor afectate definite la punctul IS.I.OR.205 litera (a) în timpul de redresare definit în prealabil de organizație.	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.	Compatibil	Lipsă
IS.I.OR.225 Răspunsul la constatările notificate de autoritatea competentă	**7. IS.I.OR.225 Răspunsul la constatările notificate de AAC**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) După primirea notificării constatărilor de la autoritatea competentă, organizația trebuie: 1. să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta; 2. să definească un plan de acțiuni corective; 3. să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către autoritatea competentă.	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.		
(b) Acțiunile menționate la litera (a) trebuie întreprinse în termenul convenit cu autoritatea competentă.	7.2. Acțiunile menționate la subpct. 7.1. trebuie întreprinse în termenul convenit cu AAC.	Compatibil	Lipsă
IS.I.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor (a) Organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite în Regulamentul (UE) nr. 376/2014 și în actele delegate și de punere în aplicare ale acestuia, dacă regulamentul respectiv îi este aplicabil.	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	informațiilor care să fie conform cu cerințele stabilite de AAC.		
(b) Fără a aduce atingere obligațiilor prevăzute în Regulamentul (UE) nr. 376/2014, 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 autorității sale competente. În plus: 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; 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.	8.2. 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.	Compatibil	Lipsă
(c) Organizația trebuie să raporteze situațiile menționate la litera (b) după cum urmează:	8.3. Organizația trebuie să raporteze situațiile menționate la subpct. 8.2. după cum urmează:	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. se transmite o notificare autorității competente 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; 2. se transmite un raport autorității competente 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 autoritatea competentă și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația; 3. se transmite autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv un raport de	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 autoritatea competentă.	Raportul de urmărire se transmite de îndată ce au fost identificate respectivele acțiuni și se întocmește în forma definită de AAC.		
IS.I.OR.235 Subcontractarea activităților de management al securității informațiilor (a) Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul 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. 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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(b) Organizația trebuie să se asigure că autoritatea competentă poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul regulament.	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.	Compatibil	Lipsă
IS.I.OR.240 Cerințele în materie de personal (a) Managerul responsabil, desemnat în conformitate cu Regulamentele (UE) nr. 1321/2014, (UE) nr. 965/2012, (UE) nr. 1178/2011, (UE) 2015/340, cu Regulamentul de punere în aplicare (UE) 2017/373 sau cu Regulamentul de punere în aplicare (UE) 2021/664, după caz, al organizației menționate la articolul 2 alineatul (1) 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: 1. să se asigure că sunt disponibile toate resursele necesare pentru a se asigura conformitatea cu cerințele prezentului 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 și 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. să stabilească și să promoveze politica de securitate a informațiilor menționată la punctul IS.I.OR.200 litera (a) subpunctul 1; 3. să demonstreze că are o înțelegere de bază a prezentului regulament.	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.		
(b) 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.	10.2. 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.	Compatibil	Lipsă
(c) Managerul responsabil trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a	10.3. Managerul responsabil trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
conformității menționată la punctul IS.I.OR.200 litera (a) subpunctul 12.	conformității menționată la subpct. 2.1.12. IS.I.OR.200.		
(d) 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.	10.4. 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.	Compatibil	Lipsă
(e) Managerul responsabil sau persoana responsabilă comună menționată la litera (d) trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea punctului IS.I.OR.200.	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.	Compatibil	Lipsă
(f) Organizația trebuie să dispună de o procedură prin care să se asigure că are suficient personal disponibil	10.6. Organizația trebuie să dispună de o procedură prin care să se asigure că are suficient personal disponibil pentru	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
pentru îndeplinirea activităților reglementate de prezenta anexă.	îndeplinirea activităților reglementate de prezenta Anexă.		
(g) Organizația trebuie să dispună de o procedură prin care să se asigure că personalul menționat la litera (f) are competența necesară pentru a-și îndeplini sarcinile.	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.	Compatibil	Lipsă
(h) Organizația trebuie să dispună de o procedură prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.	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.	Compatibil	Lipsă
(i) 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.	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.	Compatibil	Lipsă
IS.I.OR.245 Păstrarea evidențelor (a) Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor. 1. Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile: (i) orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor	**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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
în conformitate cu punctul IS.I.OR.200 litera (e); (ii) contractele pentru activitățile menționate la punctul IS.I.OR.200 litera (a) subpunctul 9; (iii) evidențele proceselor-cheie menționate la punctul IS.I.OR.200 litera (d); (iv) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.I.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.I.OR.210; (v) evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la punctele IS.I.OR.215 și IS.I.OR.230; (vi) 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.	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. Evidențele menționate la subpunctul 1 punctul (i) se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea. 3. Evidențele menționate la subpunctul 1 punctul (ii) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat. 4. Evidențele menționate la subpunctul 1 punctele (iii), (iv) și (v) se păstrează timp de cel puțin cinci ani. 5. Evidențele menționate la subpunctul 1 punctul (vi) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.	informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.		
(b) Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor. 1. Evidențele calificărilor și experienței personalului se	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația. 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.	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.		
(c) Formatul evidențelor se specifică în procedurile organizației.	11.3. Formatul evidențelor se specifică în procedurile organizației.	Compatibil	Lipsă
(d) 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.	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.	Compatibil	Lipsă
IS.I.OR.250 Manualul de management al securității informațiilor (MMSI) (a) Organizația trebuie să pună la dispoziția autorității competente un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
proceduri conexe la care se face trimitere în manualul respectiv, conținând: 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; 2. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor definite la punctul IS.I.OR.240 literele (b) și (c); 3. funcția, numele, atribuțiile, răspunderile, responsabilitățile și competența persoanei responsabile comune definite la punctul IS.I.OR.240 litera (d), dacă este cazul; 4. politica de securitate a informațiilor instituită de organizație, astfel cum este	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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
menționată la punctul IS.I.OR.200 litera (a) subpunctul 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 punctul IS.I.OR.240; 6. funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea punctului IS.I.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la punctul IS.I.OR.200 litera (a) subpunctul 12; 7. o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpunctele 2 și 6; 8. descrierea sistemului de raportare internă menționat la punctul IS.I.OR.215;	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
9. procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular: (i) documentația menționată la punctul IS.I.OR.200 litera (c); (ii) procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la punctul IS.I.OR.200 litera (a) subpunctul 9; (iii) procedura de modificare a MMSI-ului, menționată la litera (c); 10. informații detaliate referitoare la mijloace de conformare alternative aprobate în prezent.			
(b) Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de autoritatea competentă. 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 autorității competente.	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.	Compatibil	Lipsă
(c) Modificările aduse MMSI-ului se gestionează în cadrul unei proceduri instituite de organizație. Orice modificare care nu este acoperită de domeniul de aplicare al	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
acestei proceduri și orice modificare legată de modificările menționate la punctul IS.I.OR.255 litera (b) trebuie să fie aprobată de autoritatea competentă.	modificare legată de modificările menționate la subpct. 13.2. IS.I.OR.255 trebuie să fie aprobată de AAC.		
(d) 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.	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.	Compatibil	Lipsă
IS.I.OR.255 Modificări ale sistemului de management al securității informațiilor (a) Modificările aduse SMSI-ului pot fi gestionate și notificate autorității competente în cadrul unei proceduri elaborate de organizație. Procedura respectivă trebuie să fie aprobată de autoritatea competentă.	**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.	Compatibil	Lipsă
(b) În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la litera (a), organizația trebuie să solicite și să obțină o aprobare din partea autorității competente. În ceea ce privește respectivele modificări:	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite autorității competente să stabilească continuitatea conformității cu prezentul regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia; 2. organizația trebuie să pună la dispoziția autorității competente toate informațiile solicitate pentru evaluarea modificării; 3. modificarea se implementează numai după primirea unei aprobări oficiale din partea autorității competente; 4. organizația trebuie să își desfășoare activitatea în condițiile stabilite de autoritatea competentă în timpul implementării modificărilor respective.	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.		
IS.I.OR.260 Îmbunătățirea continuă (a) Organizația trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea SMSI-ului. Respectiva	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
evaluare trebuie efectuată pe baza unui calendar predefinit de organizație sau în urma unui incident de securitate a informațiilor.	organizație sau în urma unui incident de securitate a informațiilor.		
(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) 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.	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.	Compatibil	Lipsă
ANEXA III **Anexele VI (partea ARA) și VII (partea ORA) la Regulamentul (UE) nr. 1178/2011 se modifică:**			
1. Anexa VI (partea ARA) se modifică după cum urmează: (a) la punctul ARA.GEN.125 se adaugă următoarea literă (c): „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* **3.** Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la personalul navigant din aviaţia civilă, adoptat prin Hotărârea de Guvern nr. 204/2020, se modifică după cum urmează:	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203”;	3.1. Anexa nr. 6 CERINŢE APLICABILE AUTORITĂŢII AERONAUTICE CIVILE [PARTEA ARA] se completează cu pct. ARA.GEN.125 lit. (c): „(c) AAC furnizează autorității responsabile de investigarea incidentelor și accidentelor din domeniul aviației civile 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 prezentul Regulament.”;		
(b) după punctul ARA.GEN.135 se introduce punctul ARA.GEN.135A cu următorul text: „ ARA.GEN.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă 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.	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ARA.GEN.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.	(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.”;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;			
(c) la punctul ARA.GEN.200 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
informațiilor care pot avea un impact asupra siguranței aviației.”;	a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;		
(d) punctul ARA.GEN.205 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: „ ARA.GEN.205 Atribuirea de sarcini ”; (ii) se adaugă litera (c) cu următorul text: „(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORA.GEN.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că: 1. toate aspectele legate de siguranța aviației sunt coordonate și luate în	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 punctul ARA.GEN.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	(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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	de supraveghere continuă efectuate în numele său.”;		
(e) la punctul ARA.GEN.300 se adaugă litera (g) cu următorul text: „(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORA.GEN.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	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.”;	Compatibil	Lipsă
(f) după punctul ARA.GEN.330 se introduce punctul ARA.GEN.330A cu următorul text: „ ARA.GEN.330A Modificări ale sistemului de management al securității informațiilor (a) În ceea ce privește modificările gestionate și notificate autorității	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ARA.GEN.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ARA.GEN.350. (b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își	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.”;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”			
2. Anexa VII (partea ORA) se modifică după cum urmează: După punctul ORA.GEN.200 se introduce punctul ORA.GEN.200A cu următorul text: „ ORA.GEN.200A Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul ORA.GEN.200, organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	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.”	Compatibil	Lipsă
ANEXA IV **Anexa I (partea 21) la Regulamentul (UE) nr. 748/2012 se modifică după cum urmează:**			

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. Cuprinsul se modifică după cum urmează: (a) după titlul 21.B.20 se introduce următorul titlu: „21.B.20A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației”; (b) titlul punctului 21.B.30 se înlocuiește cu următorul text: „21.B.30 Atribuirea de sarcini”; (c) după titlul 21.B.240 se introduce următorul titlu: „21.B.240A Modificări ale sistemului de management al securității informațiilor”; (d) după titlul 21.B.435 se introduce următorul titlu: „21.B.435A Modificări ale sistemului de management al securității informațiilor”.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* 1.3. Se modifică titlul pct. 21.B.30: „21.B.30 Atribuirea de sarcini”;	Compatibil	Actul normativ național nu prevede Cuprins
2. La punctul 21.B.15 se adaugă litera (c) cu următorul text:	1.4. Pct. 21.B.15 se completează cu lit. (c): „**21.B.15 Informarea**	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
„(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645.”	(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.”		
3. După punctul 21.B.20 se introduce 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) Autoritatea competentă 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,	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul 21.B.15 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare.	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”	Agenției pentru Securitate Cibernetică și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.”		
4. La punctul 21.B.25 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al	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,	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
riscurilor în materie de securitate a informațiilor care pot avea un impact 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. Punctul 21.B.30 se modifică după cum urmează: (a) titlul se înlocuiește cu următorul text: „21.B.30 Atribuirea de sarcini”; (b) se adaugă litera (c) cu următorul text: „(c) Pentru certificarea și supravegherea conformității organizației cu punctele 21.A.139A și 21.A.239A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că: 1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;	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.”	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 punctul 21.B.25 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”			
6. La punctul 21.B.221 se adaugă litera (g) cu următorul text: „(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul 21.A.139A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
modificări ale domeniului de activitate al organizației.”	de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”		
7. După punctul 21.B.240 se introduce punctul 21.B.240A cu următorul text: „ 21.B.240A Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul 21.B.221. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 21.B.225. (b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul	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:	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	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.”		
8. La punctul 21.B.431 se adaugă litera (d) cu următorul text: „(d) Pentru certificarea și supravegherea conformității organizației cu punctul 21.A.239A, în plus față de respectarea dispozițiilor de la literele (a)-(c), autoritatea competentă respectă următoarele principii: 1. autoritatea competentă examinează interfețele și riscurile asociate identificate în conformitate	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
cu punctul IS.D.OR.205 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645 de fiecare organizație care face obiectul supravegherii sale; 2. dacă se constată discrepanțe în interfețele reciproce și riscurile asociate identificate de diferite organizații, autoritatea competentă 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 subpunctului 2, reiese că există riscuri semnificative asociate interfețelor cu organizații supravegheate de altă autoritate competentă din același stat membru, aceste informații se comunică autorității competente corespunzătoare.”	securitate a informațiilor cu impact potențial asupra siguranței aviației, 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.”		
9. După punctul 21.B.435 se introduce punctul 21.B.435A cu următorul text:	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**		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
„ 21.B.435A Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul 21.B.431. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 21.B.433. (b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația	(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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”		
ANEXA V **Anexele II (partea ARO) și III (partea ORO) la Regulamentul (UE) nr. 965/2012 se modifică după cum urmează:**			
1. Anexa II (partea ARO) se modifică după cum urmează: (a) la punctul ARO.GEN.125 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.”;	**4.** Regulamentul de stabilire a cerinţelor tehnice şi a procedurilor administrative referitoare la operaţiunile aeriene, adoptat prin HG nr. 612/2022, 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.	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	(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.”;		
(b) după punctul ARO.GEN.135 se introduce punctul ARO.GEN.135A cu următorul text: Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă implementează un sistem de colectare, analizare și difuzare corespunzătoare a informațiilor referitoare la incidentele și vulnerabilitățile în materie de securitate a informațiilor cu impact	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
potențial asupra siguranței aviației, care sunt raportate de organizații. Aceste activități se desfășoară în coordonare cu orice altă autoritate relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ARO.GEN.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;	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.”;		
(c) la punctul ARO.GEN.200 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	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.”;		
(d) punctul ARO.GEN.205 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: Atribuirea de sarcini”; (ii) se adaugă litera (c) cu următorul text: „(c) Pentru certificarea și supravegherea conformității organizației cu punctul ORO.GEN.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că:	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;	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 punctul ARO.GEN.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	(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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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.”;		
(e) la punctul ARO.GEN.300 se adaugă litera (g) cu următorul text: „(g) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ORO.GEN.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	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.”;	Compatibil	Lipsesc
(f) după punctul ARO.GEN.330 se introduce punctul ARO.GEN.330A cu următorul text:	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**	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ARO.GEN.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ARO.GEN.350. (b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația	(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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”		
2. Anexa III (partea ORO) se modifică după cum urmează: După punctul ORO.GEN.200 se introduce punctul ORO.GEN.200A cu următorul text: Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul ORO.GEN.200, operatorul instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	informațiilor care pot avea un impact asupra siguranței aviației.”		
ANEXA VI **Anexa II (partea ADR.AR) la Regulamentul (UE) nr. 139/2014 se modifică**			
1. La punctul ADR.AR.A.025 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.D.OR.230 din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645.”	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial 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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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. După punctul ADR.AR.A.030 se introduce punctul ADR.AR.A.030A cu următorul text: „ADR.AR.A.030A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă 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 relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori	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.	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ADR.AR.A.025 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de	(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.”		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
securitate a informațiilor asupra siguranței aviației. (d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”			
3. La punctul ADR.AR.B.005 se adaugă litera (d) cu următorul text: „(d) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	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.”	Compatibil	Lipsesc
4. Punctul ADR.AR.B.010 se modifică după cum urmează:	2.7. Se completează cu punctul ADR.AR.B.010 Atribuirea de sarcini:	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(i) titlul se înlocuiește cu următorul text: „ ADR.AR.B.010 Atribuirea de sarcini ”; (ii) se adaugă litera (c) cu următorul text: „(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ADR.OR.D.005A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă 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	„**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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
integrate în dosarele generale de certificare și de supraveghere ale organizației; 3. propriul sistem de management al securității informațiilor, instituit în conformitate cu punctul ADR.AR.B.005 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”	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.”		
5. La punctul ADR.AR.C.005 se adaugă litera (f) cu următorul text: „(f) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
ADR.OR.D.005A, în plus față de respectarea dispozițiilor de la literele (a)-(e), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”	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.”		
6. După punctul ADR.AR.C.040 se introduce punctul ADR.AR.C.040A cu următorul text: „ ADR.AR.C.040A Modificări ale sistemului de management al securității informațiilor (a) În ceea ce privește modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.D.OR.255 litera (a) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645, autoritatea competentă include examinarea acestor modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul	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	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
ADR.AR.C.005. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ADR.AR.C.055. (b) În privința altor modificări care necesită o cerere de aprobare în conformitate cu punctul IS.D.OR.255 litera (b) din anexa (partea IS.D.OR) la Regulamentul delegat (UE) 2022/1645: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	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.”		
ANEXA VII **Anexele II (partea 145), III (partea 66) și Vc (partea CAMO) la Regulamentul (UE) nr. 1321/2014 se modifică**			

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. Anexa II (partea 145) se modifică după cum urmează: (a) cuprinsul se modifică după cum urmează: (i) după titlul 145.A.200 se introduce următorul titlu: „145.A.200A Sistemul de management al securității informațiilor”; (ii) după titlul 145.B.135 se introduce următorul titlu: „145.B.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației”; (iii) titlul punctului 145.B.205 se înlocuiește cu următorul text: „145.B.205 Atribuirea de sarcini”; (iv) după titlul 145.B.330 se introduce următorul titlu: „145.B.330A Modificări ale sistemului de management al securității informațiilor”;	Regulamentul privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(b) după punctul 145.A.200 se introduce punctul 145.A.200A cu următorul text: Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul 145.A.200, organizația de întreținere instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	**145.A.200A Sistemul de management al securității informațiilor** Pe lângă sistemul de management menționat la pct. 145.A.200, organizația de întreținere instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu 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.;	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(c) la punctul 145.B.125 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.”;	**145.B.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 (partea IS.I.OR) 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	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	care pot avea un impact asupra siguranței aviației.		
(d) după punctul 145.B.135 se introduce punctul 145.B.135A cu următorul text: Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă 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 relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței	**145.B.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. 145.B.125 lit. (c și pentru furnizarea fără întârzieri nejustificate către ASC 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	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizaţiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
primite în conformitate cu punctul 145.B.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și	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 ASC și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;			
(e) la punctul 145.B.200 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	**145.B.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	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(f) punctul 145.B.205 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: Atribuirea de sarcini”; (ii) se adaugă litera (c) cu următorul text: „(c) Pentru certificarea și supravegherea conformității organizației cu punctul 145.A.200A, autoritatea competentă poate atribui sarcini entităților calificate în	**145.B.205 Atribuirea de sarcini** (c) Pentru certificarea și supravegherea conformității organizației cu pct. 145.A.200A, AAC poate atribui sarcini entităților calificate în conformitate cu lit. (a) sau oricărei autorități naționale relevante responsabile cu securitatea informațiilor sau securitatea. Atunci când atribuie sarcini, AAC se asigură că: 1. toate aspectele legate de siguranța aviației sunt coordonate și luate în	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă 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 punctul 145.B.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	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. 145.B.200 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;		
(g) la punctul 145.B.300 se adaugă litera (g) cu următorul text: „(g) În ceea ce privește certificarea și supravegherea conformității	**145.B.300 Principii de supraveghere** (g) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. 145.A.200A, în plus față de	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
organizației cu punctul 145.A.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	respectarea dispozițiilor de la lit. (a)-(f), AAC examinează orice aprobare acordată în temeiul subpct. 2.5. IS.I.OR.200 sau al suibpct. 16.5. IS.D.OR.200 din Anexa nr.2 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, în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;		produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(h) după punctul 145.B.330 se introduce punctul 145.B.330A cu următorul text: Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa	**145.B.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 cerințelor 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. 145.B.300. În cazul în care se constată o neconformitate, AAC notifică acest lucru	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
continuă, în conformitate cu principiile stabilite la punctul 145.B.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul 145.B.350. (b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	organizației, solicită modificări suplimentare și acționează în conformitate cu pct. 145.B.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 cerințelor 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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. Anexa III (partea 66) se modifică după cum urmează: (a) în cuprins, după titlul 66.B.10 se introduce următorul titlu: „66.B.15 Sistemul de management al securității informațiilor"; (b) după punctul 66.B.10 se introduce punctul 66.B.15 cu următorul text: Sistemul de management al securității informațiilor Autoritatea competentă instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației."	**66.B.15 Sistemul de management al securității informațiilor** AAC instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu 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."	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
3. Anexa Vc (partea CAMO) se modifică după cum urmează: (a) cuprinsul se modifică după cum urmează:	-	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(i) după titlul CAMO.A.200 se introduce următorul titlu: „CAMO.A.200A Sistemul de management al securității informațiilor”; (ii) după titlul CAMO.B.135 se introduce următorul titlu: „CAMO.B.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației”; (iii) titlul punctului CAMO.B.205 se înlocuiește cu următorul text: „CAMO.B.205 Atribuirea de sarcini”; (iv) după titlul CAMO.B.330 se introduce următorul titlu: „CAMO.B.330A Modificări ale sistemului de management al securității informațiilor”;			autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(b) după punctul CAMO.A.200 se introduce punctul CAMO.A.200A cu următorul text:	**CAMO.A.200A Sistemul de management al securității informațiilor** Pe lângă sistemul de management menționat la pct. CAMO.A.200,	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor și a

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul CAMO.A.200, organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	organizația instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu 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, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.		produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(c) la punctul CAMO.B.125 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203.”;	**CAMO.B.125 Informarea** (c) AAC furnizează cât mai repede posibil ASC 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 cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(d) după punctul CAMO.B.135 se introduce punctul CAMO.B.135A cu următorul text:	**CAMO.B.135A Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației**	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă 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 relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul CAMO.B.125 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie a oricăror informații, inclusiv recomandări sau măsuri	(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. CAMO.B.125 lit. (c) și pentru furnizarea fără întârzieri nejustificate ASC 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.		navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni	(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 ASC și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state vizate.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
combinate, autorităților competente ale celorlalte state membre vizate.”;			
(e) la punctul CAMO.B.200 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	**CAMO.B.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) 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.”;	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(f) punctul CAMO.B.205 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: Atribuirea de sarcini”; (ii) se adaugă litera (c) cu următorul text: „(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul CAMO.A.200A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate	**CAMO.B.205 Atribuirea de sarcini** (c) În ceea ce privește certificarea și supravegherea conformității organizației cu pct. CAMO.A.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	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor şi a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă 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 punctul CAMO.B.200 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	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. CAMO.B.200 lit. (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;		
(g) la punctul CAMO.B.300 se adaugă litera (g) cu următorul text: „(g) În ceea ce privește certificarea și supravegherea conformității	**CAMO.B.300 Principii de supraveghere** (g) În ceea ce privește certificarea și supravegherea conformității organizației	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
organizației cu punctul CAMO.A.200A, în plus față de respectarea dispozițiilor de la literele (a)-(f), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	cu pct. CAMO.A.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 stabilirea cerințelor 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.		produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri
(h) după punctul CAMO.B.330 se introduce punctul CAMO.B.330A cu următorul text: Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu	**CAMO.B.330A 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 unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la pct. CAMO.B.300. În cazul în care se constată o neconformitate, AAC notifică	Compatibil	În proces de promovare proiectul de HG privire la aprobarea Regulamentului privind continuitatea navigabilităţii aeronavelor şi a produselor, reperelor şi dispozitivelor aeronautice şi autorizarea organizațiilor și a personalului cu atribuţii în domeniu, și de abrogare a unei Hotărâri

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
principiile stabilite la punctul CAMO.B.300. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul CAMO.B.350. (b) Pentru alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu pct. CAMO.B.350. (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 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.		
ANEXA VIII **Anexele II (partea ATCO.AR) și III (partea ATCO.OR) la Regulamentul (UE) 2015/340 se modifică**			

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
1. Anexa II (partea ATCO.AR) se modifică după cum urmează: (a) la punctul ATCO.AR.A.020 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203”;	**5. Regulamentul de stabilire a cerinţelor şi procedurilor administrative referitoare la certificatele controlorilor de trafic aerian, adoptat prin Hotărârea de Guvern nr. 134/2019**, 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 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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	(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.”		
(b) după punctul ATCO.AR.A.025 se introduce punctul ATCO.AR.A.025A cu următorul text: Reacția imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației (a) Autoritatea competentă 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 relevantă responsabilă cu	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ATCO.AR.A.020 și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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 Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă ia măsuri	(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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
adecvate pentru abordarea impactului potențial al incidentului sau vulnerabilității în materie de securitate a informațiilor asupra siguranței aviației. (d) Măsurile luate în conformitate cu litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;	combinate, autorităților competente ale celorlalte state vizate.”;		
(c) la punctul ATCO.AR.B.001 se adaugă litera (e) cu următorul text: „(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	informațiilor care pot avea un impact asupra siguranței aviației.”;		
(d) punctul ATCO.AR.B.005 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: Atribuirea de sarcini”; (ii) se adaugă litera (c) cu următorul text: „(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATCO.OR.C.001A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă se asigură că: 1. toate aspectele legate de siguranța aviației sunt coordonate și luate în considerare de entitatea calificată sau de autoritatea relevantă;	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 punctul ATCO.AR.B.001 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	(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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	de supraveghere continuă efectuate în numele său.”		
(e) la punctul ATCO.AR.C.001 se adaugă litera (f) cu următorul text: „(f) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATCO.OR.C.001A, în plus față de respectarea dispozițiilor de la literele (a)-(e), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	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.”;	Compatibil	Lipsă
(f) după punctul ATCO.AR.E.010 se introduce punctul ATCO.AR.E.010A cu următorul text: Modificări ale sistemului de management al securității informațiilor	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) În ceea ce privește modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa continuă, în conformitate cu principiile stabilite la punctul ATCO.AR.C.001. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ATCO.AR.C.010. (b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare;	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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	3. dacă a constatat că organizația îndeplinește cerințele aplicabile, AAC aprobă modificarea.”		
2. Anexa III (partea ATCO.OR) se modifică după cum urmează: După punctul ATCO.OR.C.001 se introduce punctul ATCO.OR.C.001A cu următorul text: Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul ATCO.OR.C.001, organizația de pregătire instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	care pot avea un impact asupra siguranței aviației.”		
ANEXA IX **Anexele II (partea ATM/ANS.AR) și III (partea ATM/ANS.OR) la Regulamentul de punere în aplicare (UE) 2017/373 se modifică**			
1. Anexa II (partea ATM/ANS.AR) se modifică după cum urmează: (a) la punctul ATM/ANS.AR.A.020 se adaugă litera (c) cu următorul text: „(c) Autoritatea competentă a statului membru furnizează agenției 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 punctului IS.I.OR.230 din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203”;	**6. Regulamentul privind stabilirea cerințelor și procedurilor administrative pentru furnizorii de management al traficului aerian și serviciilor de navigație aeriană, adopta prin Hotărârea de Guvern nr. 119/2023,** 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 MIDR nr. 119/2020 și al actelor sale de punere în aplicare, AAC trebuie să furnizeze	Compatibil	Lipsesc

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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.”;		
(b) după punctul ATM/ANS.AR.A.025 se introduce punctul ATM/ANS.AR.A.025A cu următorul text: „ 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) Autoritatea competentă implementează un sistem de	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 relevantă responsabilă cu securitatea informațiilor sau securitatea cibernetică în interiorul statului membru, pentru a se spori coordonarea și compatibilitatea sistemelor de raportare. (b) Agenția implementează un sistem pentru analizarea corespunzătoare a oricăror informații relevante semnificative din punctul de vedere al siguranței primite în conformitate cu punctul ATM/ANS.AR.A.020 litera (c) și pentru furnizarea fără întârzieri nejustificate către statele membre și Comisie 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	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 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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
care implică produse, piese, echipamente neinstalate, persoane sau organizații supuse dispozițiilor Regulamentului (UE) 2018/1139 și ale actelor sale delegate și de punere în aplicare. (c) La primirea informațiilor menționate la literele (a) și (b), autoritatea competentă 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 litera (c) se notifică imediat tuturor persoanelor sau organizațiilor care trebuie să le respecte în temeiul Regulamentului (UE) 2018/1139 și al actelor sale delegate și de punere în aplicare. Autoritatea competentă din statul membru notifică aceste măsuri în egală măsură agenției și, atunci când sunt necesare acțiuni combinate, autorităților competente ale celorlalte state membre vizate.”;	(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.”;		
(c) la punctul ATM/ANS.AR.B.001 se adaugă litera (e) cu următorul text:	6.3. Punctul ATM/ANS.AR.B.001 se completează cu litera (e): „**ATM/ANS.AR.B.001 Sistemul de management**	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
„(e) În plus față de cerințele de la litera (a), sistemul de management instituit și menținut de autoritatea competentă trebuie să respecte anexa I (partea IS.AR) la Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	(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.”;		
(d) punctul ATM/ANS.AR.B.005 se modifică după cum urmează: (i) titlul se înlocuiește cu următorul text: „ ATM/ANS.AR.B.005 Atribuirea de sarcini ”; (ii) se adaugă litera (c) cu următorul text: „(c) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul ATM/ ANS.OR.B.005A, autoritatea competentă poate atribui sarcini entităților calificate în conformitate cu litera (a) sau oricărei autorități relevante responsabile cu	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;	Compatibil	Lipsește

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
securitatea informațiilor sau securitatea cibernetică în interiorul statului membru. Atunci când atribuie sarcini, autoritatea competentă 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 punctul ATM/ANS.AR.B.001 litera (e), acoperă toate sarcinile de certificare și de supraveghere continuă efectuate în numele său.”;	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.”;		
(e) la punctul ATM/ANS.AR.C.010 se adaugă litera (d) cu următorul text: „(d) În ceea ce privește certificarea și supravegherea conformității organizației cu punctul	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
ATM/ANS.OR.B.005A, în plus față de respectarea dispozițiilor de la literele (a)-(c), autoritatea competentă examinează orice aprobare acordată în temeiul punctului IS.I.OR.200 litera (e) din prezentul regulament sau al punctului IS.D.OR.200 litera (e) din Regulamentul delegat (UE) 2022/1645 în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.”;	(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.”;		
(f) după punctul ATM/ANS.AR.C.025 se introduce punctul ATM/ANS.AR.C.025A cu următorul text: „ATM/ANS.AR.C.025A Modificări ale sistemului de management al securității informațiilor (a) Pentru modificările gestionate și notificate autorității competente în conformitate cu procedura prevăzută la punctul IS.I.OR.255 litera (a) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203, autoritatea competentă include examinarea unor astfel de modificări în supravegherea sa	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	Compatibil	Lipsește

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
continuă, în conformitate cu principiile stabilite la punctul ATM/ANS.AR.C.010. În cazul în care se constată o neconformitate, autoritatea competentă notifică acest lucru organizației, solicită modificări suplimentare și acționează în conformitate cu punctul ATM/ANS.AR.C.050. (b) În ceea ce privește alte modificări care necesită o cerere de aprobare în conformitate cu punctul IS.I.OR.255 litera (b) din anexa II (partea IS.I.OR) la Regulamentul de punere în aplicare (UE) 2023/203: 1. la primirea cererii de efectuare a modificării, autoritatea competentă verifică dacă organizația îndeplinește cerințele aplicabile înainte de a da respectiva aprobare; 2. autoritatea competentă stabilește condițiile în care organizația își poate desfășura activitatea pe durata implementării modificării; 3. dacă a constatat că organizația îndeplinește cerințele aplicabile, autoritatea competentă aprobă modificarea.”	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. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2. Anexa III (partea ATM/ANS.OR) se modifică după cum urmează: (a) după punctul ATM/ANS.OR.B.005 se introduce punctul ATM/ANS.OR.B.005A cu următorul text: „ ATM/ANS.OR.B.005A Sistemul de management al securității informațiilor Pe lângă sistemul de management menționat la punctul ATM/ANS.OR.B.005, furnizorul de servicii instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul de punere în aplicare (UE) 2023/203, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”;	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.”;	Compatibil	Lipsă
(b) punctul ATM/ANS.OR.D.010 se înlocuiește cu următorul text: „ ATM/ANS.OR.D.010 Managementul securității (a) Furnizorii de servicii de navigație aeriană și de management	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
al fluxului de trafic aerian și administratorul rețelei, ca parte integrantă a sistemului lor de management, astfel cum se prevede la punctul 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 brețele de securitate și să alerteze	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 brețele de securitate și să alerteze personalul prin semnale de avertizare adecvate cu privire la securitate; 3. mijloacele de control al efectelor cauzate de brețele 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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 punctul ATM/ ANS.OR.B.005A.”	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.”		

Tabel de Concordanță

1. Titlul actului Uniunii Europene 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
2. Titlul proiectului de act normative național Proiectul hotărârii Guvernului cu privire la aprobarea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației
3. Gradul de compatibilitate Compatibil
4. Autoritatea/persoana responsabilă Ministerul Infrastructurii și Dezvoltării Regionale de comun cu Autoritatea Aeronautică Civilă
5. Data întocmirii/actualizării Mai 2025

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Articolul 1 Obiect În prezentul regulament sunt prevăzute cerințele care trebuie îndeplinite de organizațiile menționate la articolul 2 în vederea 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, în vederea detectării evenimentelor de securitate a informațiilor și a identificării acelora care sunt considerate incidente de securitate a informațiilor cu impact potențial asupra siguranței aviației, precum și în vederea asigurării unui răspuns la respectivele incidente de securitate a informațiilor și a redresării în urma acestora.	**Proiectul hotărârii de Guvern** **CAPITOLUL I** **OBIECTUL ȘI DOMENIU DE APLICARE** **1.** Prezentul Regulament stabilește cerințe pe care trebuie să le îndeplinească organizațiile și autoritățile competente 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.	Compatibil	Lipsă
Articolul 2 Domeniu de aplicare **(1)** Prezentul regulament se aplică următoarelor organizații: (a) organizațiilor de producție și organizațiilor de proiectare supuse	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
dispozițiilor din secțiunea A subpărțile G și J din anexa I (partea 21) la Regulamentul (UE) nr. 748/2012, cu excepția organizațiilor de proiectare și producție care sunt implicate exclusiv în proiectarea și/sau producția de aeronave ELA2, astfel cum sunt definite la articolul 1 alineatul (2) litera (j) din Regulamentul (UE) nr. 748/2012;	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, adoptat prin HG 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, adoptat prin HG nr. 91/2024;		
(b) operatorilor de aerodromuri și furnizorilor de servicii de gestionare a platformei care sunt supuși dispozițiilor din anexa III – „Partea Cerințe aplicabile organizațiilor (partea ADR.OR)” – la Regulamentul (UE) nr. 139/2014.	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, adoptat prin HG nr. 653/2018;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(2) Prezentul regulament nu aduce atingere cerințelor privind securitatea informațiilor și securitatea cibernetică stabilite la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 și la articolul 14 din Directiva (UE) 2016/1148.	**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.	Compatibil	Lipsă
Articolul 3 Definiții 1. „securitate a informațiilor” înseamnă păstrarea confidențialității, integrității, autenticității și disponibilității rețelelor și sistemelor informatice; 2. „eveniment de securitate a informațiilor” înseamnă 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. „incident” înseamnă orice eveniment care are un efect negativ asupra securității rețelelor și sistemelor informatice, astfel cum este definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148;	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
4. „risc în materie de securitate a informațiilor” înseamnă riscul la adresa organizării operațiunilor de aviație civilă, precum și la adresa activelor, persoanelor fizice și a altor organizații, atribuibil 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; 5. „amenințare” înseamnă o încălcare potențială a securității informațiilor care există atunci când o entitate, o circumstanță, o acțiune sau un eveniment ar putea cauza prejudicii; 6. „vulnerabilitate” înseamnă 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.	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.		
Articolul 4 Cerințe care decurg din alte acte legislative ale Uniunii	-	Norme UE neaplicabile	Prevederi tranzitorii în contextul în care Directiva

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(1) Atunci când o organizație menționată la articolul 2 îndeplinește cerințe de securitate stabilite la articolul 14 din Directiva (UE) 2016/1148 care sunt echivalente cu cerințele stabilite în prezentul regulament, se consideră că îndeplinirea respectivelor cerințe de securitate constituie îndeplinirea cerințele stabilite în prezentul regulament.			(UE) 2016/1148 a fost abrogată
(2) În cazul în care o organizație menționată la articolul 2 este un operator sau o entitate menționată în programele naționale de securitate a aviației civile ale statelor membre, stabilite în conformitate cu articolul 10 din Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului ([8]), cerințele de securitate cibernetică de la punctul 1.7 din anexa la Regulamentul de punere în aplicare (UE) 2015/1998 sunt considerate echivalente cu cerințele stabilite în prezentul regulament, cu excepția punctului IS.D.OR.230 din anexa la prezentul regulament, care trebuie respectat.	-	Norme UE neaplicabile	Prevederi tranzitorii în contextul în care Directiva (UE) 2016/1148 a fost abrogată
(3) După consultarea AESA și a grupului de cooperare menționat la articolul 11 din Directiva (UE)	-	Norme UE neaplicabile	Prevederi tranzitorii în contextul în care Directiva

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
2016/1148, Comisia poate să emită orientări pentru evaluarea echivalenței cerințelor stabilite în prezentul regulament cu cerințele stabilite în Directiva (UE) 2016/1148.			(UE) 2016/1148 a fost abrogată
Articolul 5 Autoritatea competentă **(1)** Autoritatea responsabilă cu certificarea și supravegherea respectării prezentului regulament este: (a) în ceea ce privește organizațiile menționate la articolul 2 litera (a), autoritatea competentă desemnată în conformitate cu anexa I (partea 21) la Regulamentul (UE) nr. 748/2012;	**4.** Autoritatea responsabilă de supravegherea şi controlul respectării prevederilor prezentului Regulament de către organizaţiile menţionate la pct. 2 este autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile - *Autoritatea Aeronautică Civilă (în continuare – „AAC”).*	Compatibil	Lipsă
(b) în ceea ce privește organizațiile menționate la articolul 2 litera (b), autoritatea competentă desemnată în conformitate cu anexa III (partea ADR.OR) la Regulamentul (UE) nr. 139/2014.	**4.** Autoritatea responsabilă de supravegherea şi controlul respectării prevederilor prezentului Regulament de către organizaţiile menţionate la pct. 2 este autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile - *Autoritatea Aeronautică Civilă (în continuare – „AAC”).*	Compatibil	Lipsă
(2) În sensul prezentului regulament, statele membre pot desemna o entitate independentă și autonomă care să îndeplinească rolul și responsabilitățile atribuite	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
autorităților competente menționate la alineatul (1). În acest caz, trebuie stabilite măsuri de coordonare între entitatea respectivă și autoritățile competente, astfel cum se menționează la alineatul (1), pentru a se asigura supravegherea efectivă a tuturor cerințelor care trebuie respectate de către organizație.	Securitatea Cibernetică (în continuare „ASC”), în conformitate cu prevederile Regulamentului cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, adoptat prin Hotărârea de Guvern nr. 1028/2023 și altor acte conexe.		
Articolul 6 Modificări aduse Regulamentului (UE) nr. 748/2012 **Anexa I (partea 21) la Regulamentul (UE) nr. 748/2012** se modifică după cum urmează: **1.** cuprinsul se modifică după cum urmează: (a) după titlul 21.A.139 se introduce titlul următor: „21.A.139A Sistemul de management al securității informațiilor”; (b) după titlul 21.A.239 se introduce titlul următor:	-	Prevederi UE neaplicabile	Actul normativ național – HG nr. 91/2024 nu conține Cuprins.

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
„21.A.239A Sistemul de management al securității informațiilor”;			
2. după punctul 21.A.139 se introduce următorul punct 21.A.139A: „21.A.139A Sistemul de management al securității informațiilor Pe lângă sistemul de management al producției prevăzut la punctul 21.A.139, organizația de producție instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul delegat (UE) 2022/1645 al Comisiei (*1), pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației.* **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, adoptat prin HG nr. 91/2024, 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 pct. 21.A.139 se completează cu pct. 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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.”;		
3. după punctul 21.A.239 se introduce următorul punct 21.A.239A: „21.A.239A Sistemul de management al securității informațiilor Pe lângă sistemul de management al proiectării prevăzut la punctul 21.A.239, organizația de proiectare instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu Regulamentul delegat (UE) 2022/1645, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* 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: 1.2. după pct. 21.A.239 se completează cu pct. 21.A.239A: „**21.A.239A Sistemul de management al securității informațiilor** Pe lângă sistemul de management al proiectării prevăzut la punctul 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	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.”.		
Articolul 7 **Modificări aduse Regulamentului (UE) nr. 139/2014** Anexa III (partea ADR.OR) la Regulamentul (UE) nr. 139/2014 se modifică după cum urmează: **1.** după punctul ADR.OR.D.005 se introduce următorul punct ADR.OR.D.005A: „ADR.OR.D.005A Sistemul de management al securității informațiilor Operatorul de aerodrom instituie, implementează și menține un sistem de management al securității informațiilor în conformitate cu	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* **2.** Regulamentul privind procedurile administrative referitoare la aerodromuri, adoptat prin Hotărârea de Guvern nr. 653/2018, 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Regulamentul delegat (UE) 2022/1645 al Comisiei (*2), pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.	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. punctul ADR.OR.D.007 se înlocuiește cu următorul text: „ADR.OR.D.007 Managementul datelor aeronautice și al informațiilor aeronautice (a) În cadrul sistemului său de management, operatorul de aerodrom 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 stabilește un sistem de	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* 2.2. Prevederile pct. ADR.OR.D.007 se înlocuiește cu următorul text: „**ADR.OR.D.007 Managementul datelor aeronautice și al informațiilor aeronautice** (a) În cadrul sistemului său de management, operatorul de aerodrom/aerodrom 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 brețele de securitate și să alerteze personalul prin avertizări adecvate cu privire la securitate; (3) mijloacele de control al efectelor cauzate de brețele de securitate și de identificare a măsurilor de remediere și a procedurilor de reducere a riscurilor pentru prevenirea repetării acestora.	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 brețele de securitate și să alerteze personalul prin avertizări adecvate cu privire la securitate; (3) mijloacele de control al efectelor cauzate de brețele 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 punctul ADR.OR.D.005A.”.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(d) Operatorul de aerodrom 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 punctul ADR.OR.D.005A.”;			
3. după punctul ADR.OR.F.045 se introduce următorul punct 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 delegat (UE) 2022/1645, pentru a asigura managementul corespunzător al riscurilor în materie de securitate a informațiilor care pot avea un impact asupra siguranței aviației.”	**Anexa nr. 3** *La Regulamentul privind stabilirea cerințelor referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației* 2.3. După prevederile pct. ADR.OR.F.045 se introduce următorul pct. 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
	securitate a informațiilor care pot avea un impact asupra siguranței aviației.”.		
Articolul 8 Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*. Se aplică de la 16 octombrie 2025. Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre. Adoptat la Bruxelles, 14 iulie 2022.	**Proiectul hotărârii de Guvern** **3.** Prevederile pct. 1, subpct. 1.1 și 1.2, ale pct. 2 subpct. 2.1, 2.2 și 2.3 din Anexa nr. 3 la Regulament intră în vigoare la 16 octombrie 2025.	Compatibil	Lipsă
ANEXĂ **SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE ORGANIZAȚIEI [PARTEA-IS.D.OR]**			
IS.D.OR.100 Domeniul de aplicare Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la articolul 2 din prezentul regulament.	**Anexa nr. 2** **[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.	Compatibil	Lipsă
IS.D.OR.200 Sistemul de management al securității informațiilor (SMSI)	**16. IS.D.OR.200 Sistemul de management al securității informațiilor (SMSI)** **16.1.** Pentru a atinge obiectivele prevăzute la pct. 1 din Regulament,	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(a) Pentru a atinge obiectivele prevăzute la articolul 1, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația: (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) identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.205; (3) definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.210; (4) implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.215;	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;		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(5) definește și implementează, în conformitate cu punctul 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 punctului IS.D.OR.205 litera (e), asigură un răspuns la respectivele incidentele de securitate a informațiilor și se redresează în urma acestora; (6) implementează măsurile care au fost notificate de autoritatea competentă ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației; (7) ia măsurile corespunzătoare, în conformitate cu punctul IS.D.OR.225, pentru abordarea constatărilor notificate de autoritatea competentă; (8) implementează un sistem de raportare externă în conformitate cu punctul IS.D.OR.230, astfel încât autoritatea competentă să poată lua măsuri corespunzătoare;	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(9) îndeplinește cerințele de la punctul IS.D.OR.235 când subcontractează altor organizații orice parte a activităților menționate la punctul IS.D.OR.200; (10) îndeplinește cerințele în materie de personal stabilite la punctul IS.D.OR.240; (11) îndeplinește cerințele de păstrare a evidențelor stabilite la punctul IS.D.OR.245; (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; (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.	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1, organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.D.OR.260.	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.	Compatibil	Lipsă
(c) Organizația trebuie să documenteze, în conformitate cu punctul IS.D.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.D.OR.200 litera (a) și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu punctul IS.D.OR.255.	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.	Compatibil	Lipsă
(d) Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma punctului IS.D.OR.200 litera (a) 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.	16.4. 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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(e) Fără a se aduce atingere obligației de conformitate cu cerințele de raportare prevăzute în Regulamentul (UE) nr. 376/2014 al Parlamentului European și al Consiliului (1) și cu cerințele de la punctul IS.D.OR.200 litera (a) subpunctul (13), organizația poate primi din partea autorității competente aprobarea de a nu implementa cerințele menționate la literele (a)-(d) și cerințele conexe prevăzute la punctele IS.D.OR.205 – IS.D.OR.260, dacă demonstrează într-un mod considerat satisfăcător de autoritatea respectivă 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 punctul IS.D.OR.205 și examinată și aprobată de autoritatea sa competentă.	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
Menținerea valabilității respectivei aprobări va fi examinată de autoritatea competentă în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.	și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.		
IS.D.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor **(a)** Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă: (1) activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația; (2) echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpunctul (1).	**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.	Compatibil	Lipsă
(b) 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.	17.2. 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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) În ceea ce privește elementele și interfețele menționate la literele (a) și (b), organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie: (1) să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație; (2) să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu literele (a) și (b). Clasificarea predefinită menționată la subpunctul (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	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
tratat în conformitate cu punctul IS.D.OR.210. Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în temeiul subpunctului (1) se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).			
(d) Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și (c) în oricare dintre următoarele situații: (1) când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor; (2) când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații; (3) când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(4) analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.			
IS.D.OR.210 Tratarea riscurilor în materie de securitate a informațiilor **(a)** Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.D.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației: (1) să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare; (2) să diminueze consecințele asupra siguranței aviației, asociate materializării scenariului de amenințare; (3) să evite riscurile. Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.	**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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(b) Persoana menționată la punctul IS.D.OR.240 literele (a) și (b) și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul 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 punctul IS.D.OR.205 litera (b) cu privire la orice risc comun celor două organizații.	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.	Compatibil	Lipsă
IS.D.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor (a) 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 punctului IS.D.OR.230.	**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.	Compatibil	Lipsă
(b) Sistemul respectiv și procesul menționat la punctul IS.D.OR.220 trebuie să îi permită organizației:	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(1) să identifice care dintre evenimentele raportate în temeiul literei (a) sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației; (2) să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul (1) și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu punctele IS.D.OR.205 și IS.D.OR.220; (3) să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu subpunctul (1); (4) să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.	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.		
(c) Orice organizație subcontractată care ar putea expune organizația la riscuri în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației are	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 litera (b).	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.		
(d) Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.	19.4. Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.	Compatibil	Lipsă
(e) Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.	19.5. Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.	Compatibil	Lipsă
IS.D.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare (a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.D.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul 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	**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:	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
măsuri de detectare trebuie să permită organizației: (1) să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale; (2) să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.	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.		
(b) Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Aceste măsuri de răspuns trebuie să permită organizației: (1) să declanșeze reacția la avertizările menționate la litera (a) subpunctul (2) prin activarea unor resurse și planuri de acțiune predefinite; (2) să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare; (3) să controleze modul de defectare al elementelor afectate definite la punctul IS.D.OR.205 litera (a).	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(c) 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: (1) să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil; (2) să asigure atingerea unei stări de siguranță a elementelor afectate definite la punctul IS.D.OR.205 litera (a) în timpul de redresare definit în prealabil de organizație.	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.	Compatibil	Lipsă
IS.D.OR.225 Răspunsul la constatările notificate de autoritatea competentă (a) După primirea notificării constatărilor de la autoritatea competentă, organizația trebuie: (1) să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta; (2) să definească un plan de acțiuni corective;	**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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(3) să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către autoritatea competentă.			
(b) Acțiunile menționate la litera (a) trebuie întreprinse în termenul convenit cu autoritatea competentă.	21.2. Acțiunile menționate la subpct. 21.1. trebuie întreprinse în termenul convenit cu AAC.	Compatibil	Lipsă
IS.D.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor (a) Organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite în Regulamentul (UE) nr. 376/2014 și în actele delegate și de punere în aplicare ale acestuia, dacă regulamentul respectiv îi este aplicabil.	**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.	Compatibil	Lipsă
(b) Fără a aduce atingere obligațiilor prevăzute în Regulamentul (UE) nr. 376/2014, 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 autorității sale competente. În plus: (1) atunci când un astfel de incident sau o astfel de vulnerabilitate	22.2. Fără a aduce atingere obligațiilor prevăzute în Reglementarea aeronautică civilă „Regulamentul privind raportarea, analiza și 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:	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
afectează o aeronavă ori un sistem sau o componentă asociată, organizația trebuie să raporteze acest lucru și titularului aprobării de proiect; (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.	22.2.1. 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.		
(c) Organizația trebuie să raporteze situațiile menționate la litera (b) după cum urmează: (1) se transmite o notificare autorității competente 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; (2) se transmite un raport autorității competente 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	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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 autoritatea competentă și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația; (3) se transmite autorității competente 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	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.		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
în forma definită de autoritatea competentă.			
IS.D.OR.235 Subcontractarea activităților de management al securității informațiilor (a) Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul 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. 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.	Compatibil	Lipsă
(b) Organizația trebuie să se asigure că autoritatea competentă poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul regulament.	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.	Compatibil	Lipsă
IS.D.OR.240 Cerințele în materie de personal (a) Managerul responsabil al organizației sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare, desemnat în conformitate cu Regulamentul	**24. IS.D.OR.240 Cerințele în materie de personal** 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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(UE) nr. 748/2012 și cu Regulamentul (UE) nr. 139/2014, astfel cum se menționează la articolul 2 alineatul (1) literele (a) și (b) 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: (1) să se asigure că sunt disponibile toate resursele necesare pentru a se conforma cerințelor prezentului regulament; (2) să stabilească și să promoveze politica de securitate a informațiilor menționată la punctul IS.D.OR.200 litera (a) subpunctul (1); (3)să demonstreze că deține cunoștințe de bază privind prezentul regulament.	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.		
(b) 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	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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.	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.		
(c) 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 punctul IS.D.OR.200 litera (a) subpunctul (12).	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.	Compatibil	Lipsă
(d) 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	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
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.	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.		
(e) Managerul responsabil sau șeful organizației de proiectare ori persoana responsabilă comună menționată la litera (d) trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea punctului IS.D.OR.200.	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.	Compatibil	Lipsă
(f) Organizația trebuie să dispună de un proces prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta anexă.	24.6. Organizația trebuie să dispună de un proces prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta Anexă.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(g) Organizația trebuie să dispună de un proces prin care să se asigure că personalul menționat la litera (f) are competența necesară pentru a-și îndeplini sarcinile.	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.	Compatibil	Lipsă
(h) Organizația trebuie să dispună de un proces prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.	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.	Compatibil	Lipsă
(i) 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.	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.	Compatibil	Lipsă
IS.D.OR.245 Păstrarea evidențelor (a) Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor. (1) Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile: (i) orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor	**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;	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
în conformitate cu punctul IS.D.OR.200 litera (e); (ii) contractele pentru activitățile menționate la punctul IS.D.OR.200 litera (a) subpunctul (9); (iii) evidențele proceselor-cheie menționate la punctul IS.D.OR.200 litera (d); (iv) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.D.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.D.OR.210; (v) evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la punctele IS.D.OR.215 și IS.D.OR.230; (vi) 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.	25.1.1.4. 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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(2) Evidențele menționate la subpunctul (1) punctul (i) se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea. (3) Evidențele menționate la subpunctul (1) punctul (ii) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat. (4) Evidențele menționate la subpunctul (1) punctele (iii), (iv) și (v) se păstrează timp de cel puțin cinci ani. (5) Evidențele menționate la subpunctul (1) punctul (vi) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.	definită în cadrul unei proceduri instituite de organizație.		
(b) Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor. (1) Evidențele calificărilor și experienței personalului se	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația. (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.	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.		
(c) Formatul evidențelor se specifică în procedurile organizației.	25.3. Formatul evidențelor se specifică în procedurile organizației.	Compatibil	Lipsă
(d) 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.	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.	Compatibil	Lipsă
IS.D.OR.250 Manualul de management al securității informațiilor (MMSI) (a) Organizația trebuie să pună la dispoziția autorității competente un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și	**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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
proceduri conexe la care se face trimitere în manualul respectiv, conținând: (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; (2) funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor menționate la punctul IS.D.OR.240 literele (b) și (c); (3) funcția, numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei responsabile comune menționate la punctul IS.D.OR.240 litera (d), dacă este cazul;	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(4) politica de securitate a informațiilor instituită de organizație, astfel cum este menționată la punctul IS.D.OR.200 litera (a) subpunctul (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 punctul IS.D.OR.240 litera (d); (6) funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea punctului IS.D.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la punctul IS.D.OR.200 litera (a) subpunctul (12); (7) o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpunctele (2) și (6);	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		

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(8) descrierea sistemului de raportare internă menționat la punctul IS.D.OR.215; (9) procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular: (i) documentația menționată la punctul IS.D.OR.200 litera (c); (ii) procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la punctul IS.D.OR.200 litera (a) subpunctul (9); (iii) procedura de modificare a MMSI-ului, definită la litera (c); (10) informații detaliate referitoare la mijloace de conformare alternative aprobate în prezent.	conformitate (AltMoC) aprobate în prezent.		
(b) Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de autoritatea competentă. MMSI-ul trebuie modificat în funcție de necesități, astfel încât să reprezinte o descriere actualizată a SMSI-ului	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	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
organizației. O copie a oricăror modificări aduse MMSI-ului trebuie transmisă autorității competente.	oricăror modificări aduse MMSI-ului trebuie transmisă AAC.		
(c) 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 punctul IS.D.OR.255 litera (b) trebuie să fie aprobată de autoritatea competentă.	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.	Compatibil	Lipsă
(d) 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.	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.	Compatibil	Lipsă
IS.D.OR.255 Modificări ale sistemului de management al securității informațiilor (a) Modificările aduse SMSI-ului pot fi gestionate și notificate autorității competente în cadrul unei proceduri elaborate de organizație. Procedură respectivă trebuie să fie aprobată de autoritatea competentă.	**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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
(b) În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la litera (a), organizația trebuie să solicite și să obțină o aprobare din partea autorității competente. În ceea ce privește aceste modificări: (1) cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite autorității competente să stabilească continuitatea conformității cu prezentul regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia; (2) organizația trebuie să pună la dispoziția autorității competente toate informațiile solicitate pentru evaluarea modificării; (3) modificarea se implementează numai după primirea unei aprobări oficiale din partea autorității competente; (4) organizația trebuie să își desfășoare activitatea în condițiile stabilite de autoritatea competentă	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.	Compatibil	Lipsă

6. Actul Uniunii Europene	7. Proiectul de act normativ național	8. Gradul de compatibilitate	9. Observațiile
în timpul implementării modificărilor respective.			
IS.D.OR.260 Îmbunătățirea continuă (a) 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. 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.	Compatibil	Lipsă
(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) 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.	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.	Compatibil	Lipsă