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