



CIRCULARĂ DE AERONAUTICĂ CIVILĂ

Domeniu:	GENERAL	Data:	ianuarie 2026	Cod:	CA: ISMM-CL-01
----------	---------	-------	------------------	------	----------------

**MANUALUL DE MANAGEMENT AL SECURITĂȚII INFORMAȚIILOR
(ISMM)
- CHECK-LIST-**



**MANUALUL DE MANAGEMENT AL
SECURITĂȚII INFORMAȚIILOR
(ISMM)**

ianuarie
2026

Pag. 3 din 6

CUPRINS

1. INTRODUCERE.....	4
2. SCOP	4
3. APLICABILITATE.....	4
4. REFERINȚE ACTE NORMATIVE ȘI PROCEDURALE	4
5. PREVEDERI ȘI MOD DE APLICARE	5
6. MENȚIUNI	5
7. FORMULARE	5
8. ANEXE	5



1. INTRODUCERE

Prezenta circulară de aeronautică civilă este emisă pentru informare și orientare. Descrie un exemplu al unui mijloc acceptabil de conformare, în scopul de a demonstra îndeplinirea cerințelor reglementărilor și standardelor aplicabile. Această circulară de aeronautică civilă, așa cum este redactată, nu modifică, conduce sau permite abateri de la cerințele reglementărilor aplicabile.

2. SCOP

Prezenta circulară introduce în aplicare:

- documentul "Check-list ISMM" cod formular F-CA-ISMM-CL-01. Scopul acestuia este furnizarea unui instrument pentru facilitarea documentării conformării manualului de management al securității informațiilor cu cerințele de reglementare aplicabile. În scopul standardizării și pentru a facilita întocmirea ISMM de către organizații; AACR recomandă utilizarea prezentului document pentru dezvoltarea procedurilor ISMM".
- cererea de scutire de la aplicarea anumitor cerințe ale regulamentelor nr. (UE) 2023/203 și (UE) 2022/1645 (Partea IS), în conformitate cu IS.I/D.OR-200 (e). cod formular F-CA-ISMM-DR-01

3. APLICABILITATE

Prevederile prezentei circulare de navigabilitate sunt aplicabile:

- Organizațiilor din domeniile AIR și OPS menționate la art. 2 din Regulamentul (UE) nr. 2023/203 și la art. 2 din Regulamentul (UE) nr. 2022/1645 pentru care AACR este autoritate competentă – ca material de îndrumare și autoevaluare pentru întocmirea ISMM,
- AACR – ca document de verificare utilizat în procesul de aprobare a ISMM.

4. REFERINȚE ACTE NORMATIVE ȘI PROCEDURALE

- Regulamentul de punere în aplicare **(UE) 2023/203** 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,[...]
- Regulamentul delegat (UE) 2022/1645 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, [...]

5. PREVEDERI ȘI MOD DE APLICARE

- 5.1. Documentul "Check-list ISMM" cod formular F-CA-ISMM-CL-01 ed.1/2026, introdus prin prezenta circulară, este derivat din cerințele prevăzute în reglementările (UE) 2022/1645 și (UE) 2023/203, Anexa II - PART IS și a AMC/ GM aferente. Este conceput pe secțiuni, astfel încât să poată fi utilizat atât ca material de ghidare pentru întocmirea ISMM de către organizații, cât și ca document de verificare a conținutului acestuia în raport cu cerințele de reglementare.
- 5.2. Documentul asigură o înregistrare metodică a conformării conținutului manualului cu cerințele de reglementare aplicabile, permițând astfel o evaluare rapidă și exactă a acestuia de către organizații (în procesul de aprobare internă a ISMM) și de către AACR.
- 5.3. Secțiunea 3 "Evaluare conținut ISMM" a documentului "Check-list ISMM" completată de către managerul de monitorizarea conformării din cadrul organizației se transmite la AACR odată cu manualul sau amendamente ale acestuia.

6. MENȚIUNI

Formularele F-CA-ISMM-CL-01 și F-CA-ISMM-DR-01 sunt postate pe site-ul AACR: www.caa.ro la secțiunea "LEGISLAȚIE GENERALĂ"

7. FORMULARE

- 7.1. F-CA-ISMM-CL-01 ed.1/2026 Check-list ISMM
- 7.2. F-CA-ISMM-DR-01 ed.1/2026 Cerere de scutire de la aplicarea anumitor cerințe ale regulamentelor nr. (UE) 2023/203 și (UE) 2022/1645 (Partea IS), în conformitate cu IS.I/D.OR-200 (e)

8. ANEXE

NA



CIRCULARĂ DE AERONAUTICĂ CIVILĂ

CA: ISMM-CL-01

**MANUALUL DE MANAGEMENT AL
SECURITĂȚII INFORMAȚIILOR
(ISMM)**

ianuarie
2026

Pag. 6 din 6

PENTRU INFORMAȚII SUPLIMENTARE CONTACTAȚI:

AUTORITATEA AERONAUTICĂ CIVILĂ ROMÂNĂ

Șos. București-Ploiești nr.38-40, București, RO-013695

tel. +40 21 208 15 21, fax +40 21 208 15 35,

e-mail: contact@caa.ro

**Sugestii de amendare la prezenta circulară de aeronautică civilă
pot fi transmise la AACR, via e-mail, la una din adresele:**

contact@caa.ro sau registratura@caa.ro

CHECK-LIST ISMM

Secțiunea 1. GENERALITĂȚI

1.1 Scop și aplicabilitate

Scopul prezentului document este furnizarea unui instrument pentru facilitarea documentării conformării manualului de management al securității informațiilor (ISMM) cu cerințele de reglementare aplicabile. Prezentul document este complementar cerințelor regulamentelor (UE) 2023/203, Anexa II - Part-IS.I.OR și (UE) 2022/1645 Anexa-Part-IS.D.OR - Managementul riscurilor de securitate a informațiilor cu potențial impact asupra siguranței cu modificările și completările ulterioare și nu înlocuiește, nu modifică, nu generează și nu permite abateri de la cerințele definite în regulament.

Documentul include informațiile relevante conținute în IS.I/D.OR.250 și AMC/GM aferente, cuprinzând pentru fiecare capitol un conținut minim al subiectelor ce trebuie tratate în cadrul ISMM.

Documentul este destinat:

- Organizațiilor menționate la art. 2 din Regulamentul (UE) nr. 2023/203 și la art. 2 din Regulamentul (UE) nr. 2022/1645 pentru care AACR este autoritate competentă (numite în continuare "Organizații") – ca material de îndrumare pentru întocmirea ISMM,
- AACR – ca document de verificare utilizat în procesul de aprobare a ISMM, pe parcursul activității de certificare și supraveghere continuă.

1.2 Instrucțiuni de completare

Organizația completează **Secțiunea 3**, după cum urmează:

- Informații generale referitoare la organizație, referință nr. autorizare, etc
- în rubrica "**Conf.**" se bifează capitolele/subcapitolele care au fost abordate/ supuse modificării. în cazul în care anumite secțiuni/ capitole nu sunt aplicabile în cadrul organizației în rubrica "Observații/ Ref. ISMM". se notează cu N/A.,
- în rubrica "**Observații / Ref. ISMM**" se înregistrează referințe din manual și/sau la alte la proceduri dezvoltătoare, instrucțiuni sau alte documente, anexe, formulare asociate, la liste care sunt gestionate separat și orice alte observații considerate necesare pentru a documenta conformarea
- managerul monitorizarea conformării semnează și datează finalizarea evaluării interne.

Notă: Paginile relevante ale **Secțiunii 3** a prezentului document, completate corespunzător, se transmit la AACR odată cu manualul de management al securității informațiilor (ISMM) sau amendamente ale acestuia.

Rubrica "**AACR**" din **Secțiunea 3** este utilizată de inspectorii AACR pentru înregistrarea rezultatului analizei conformării conținutului ISMM cu prevederile reglementării. AACR bifează cu V pentru conformare, X pentru neconformare și NA în cazul în care anumite secțiuni/ capitole nu sunt aplicabile în cadrul organizației. **Secțiunea 4** "Rezultatul evaluării AACR a conformării conținutului ISMM cu cerințele de reglementare aplicabile", este completată de inspectorii AACR, ca o concluzie a evaluării efectuată asupra manualului transmis spre aprobare.

Secțiunea 2. ISMM

În scopul standardizării și pentru a facilita întocmirea ISMM de către organizație, AACR recomandă utilizarea prezentului document pentru dezvoltarea procedurilor ISMM. AACR recomandă integrarea ISMS în cadrul sistemului de management al siguranței existent (SMS). Mai jos sunt prezentate exemple de elemente comune ambelor sisteme:

- Angajamentul managementului
- Politici și proceduri
- Managementul riscurilor
- Păstrarea înregistrărilor
- Instruire și conștientizare
- Audituri și evaluări
- Comunicare cu părțile interesate (raportare internă și externă)
- Raportare și îmbunătățire continuă

Indiferent de modul în care organizația alege să documenteze ISMS (într-un manual independent, în manualul sistemului de management integrat sau în alte manuale ale organizației aprobate de AACR - memoriile de prezentare a organizației, Manual de Operațiuni, CAME, MOE, etc.), organizația trebuie să particularizeze manualul pentru a descrie cât mai fidel practicile și procedurile proprii, adăugând pagini și/sau paragrafe, după cum este necesar pentru demonstrarea conformării cu cerințele PART IS.

Notă 1: Termenul ISMM este utilizat în această circulară ca denumire generică pentru orice manual care conține procedurile ISMS, indiferent de denumirea adoptată de organizație.

Organizația poate alege să utilizeze un alt format decât cel descris în prezentul document atât timp cât toate secțiunile aplicabile ale reglementării sunt tratate și referite.

Modul de întocmire al procedurilor detaliate descrise în ISMM, trebuie să respecte politicile organizației cu privire la redactarea și gestionarea documentelor. Organizația trebuie să întocmească procedurile astfel încât acestea să poată răspunde precis la următoarele întrebări: **ce trebuie făcut? cine face? când face? unde face? cu ce face? cum face? ce înregistrări/formulare utilizează?**

O structura posibilă a unei proceduri poate fi: **scop, domeniu, terminologie și abrevieri, documente de referință, descrierea procedurii, înregistrări / formulare, responsabilități, anexe.**

2.1 Formatul ISMM

ISMM poate fi întocmit în format electronic sau pe hârtie.

Recomandări:

Pentru varianta pe hârtie: utilizarea hârtiei albe format A4, îndosariere cu separatoare de capitole.

Pentru formatul electronic: format .pdf.

Limba utilizată pentru întocmirea acestuia poate fi limba română sau limba engleză.

2.2 Structura ISMM

Manualul poate fi întocmit ca un document unic sau poate consta în mai multe documente separate, organizarea manualului rămâne la latitudinea organizației.

Ca document unic, ISMM, întocmit conform cerințelor IS.I/D.OR.250, trebuie să conțină toate informațiile solicitate pentru a demonstra conformarea cu reglementările aplicabile, inclusiv procedurile detaliate ale sistemului de securitatea informației.

În cazul în care ISMM se constituie în mai multe documente separate, acesta trebuie să conțină informațiile solicitate în IS.I/D.OR.250 și o descriere sumară a modului în care se asigură conformarea cu cerințele regulamentului, în celelalte capitole. Materialele adiționale (liste, proceduri asociate) publicate ca documente separate, trebuie să fie referite în ISMM.

În acest caz:

- ISMM trebuie să conțină referințe încrucișate la proceduri, documente, anexe, formulare asociate sau la liste care sunt gestionate separat
- Toate documentele asociate trebuie să îndeplinească aceleași cerințe ca cele descrise pentru ISMM și trebuie supuse aprobării AACR odată cu ISMM.
- ISMM va conține un minim de informații care să demonstreze conformarea cu reglementările aplicabile. Un capitol ISMM care doar referă o procedură asociată nu este acceptabil.

2.3 Gestionarea ISMM

Pentru monitorizarea corespunzătoare a aprobării este esențial ca organizația să identifice clar atât ediția inițială a manualului cât și toate amendamentele ulterioare. Orice modificare a ISMM aprobat trebuie să fie identificată prin:

- Un nou număr al ediției și/sau reviziei;
- O nouă dată a ediției și/sau reviziei;
- Marcarea clară a textului modificat în cadrul fiecărui capitol (ex. Utilizând bare verticale, punând în evidență cu o anumită culoare textul modificat, etc).

ISMM trebuie să detalieze metodele stabilite pentru identificarea modificărilor manualului.

Exemple:

1. ISMM identificat cu număr de ediție și număr de revizie

În acest caz, la fiecare modificare a ediției, numărul reviziei pornește din nou de la "0". Procedura descrisă în ISMM va menționa criteriile de creștere a numărului ediției. Se pot adopta diverse criterii cum ar fi:

- la "x" revizii se crește numărul ediției manualului, sau
- la modificarea a 25% din conținut se crește numărul ediției, sau

- modificările minore sunt identificate prin modificarea numărului reviziei iar modificările majore prin modificarea numărului ediției, etc

Număr ediție	Data ediției	Număr revizie	Data revizie
1 (inițială)	01/01/2025	0	01/01/2025
		1	17/02/2025
		2	25/10/2025
2	20/11/2025	0	20/11/2025
		1	05/03/2025
		2	15/08/2025

2. ISMM identificat doar cu numărul reviziei (sau ediției). Această soluție este mai puțin flexibilă având în vedere că orice modificare a ISMM va fi identificată doar prin modificarea numărului reviziei (sau ediției).

Fiecare pagină a ISMM trebuie identificată după cum urmează:

- Numele organizației
- Numele documentului (ISMM)
- Numărul ediției / reviziei ISMM și data
- Capitolul ISMM
- Numărul paginii

La începutul volumului, prima pagină a ISMM trebuie să specifice:

- Manualul de management al securității informațiilor (ISMM) și codul documentului
- Numele organizației (așa cum e definit în certificatul de autorizare)
- Adresa, telefon, fax al sediului social al organizației
- Numărul exemplarului ISMM conform listei de distribuție
- Referința documentelor de certificare deținute de organizație
- Aprobarea internă a documentului

Ediția inițială a manualului trebuie transmisă spre aprobare la AACR. Transmiterea inițială a acestuia, precum și corespondența ulterioară referitoare la neconformitățile constatate și remedierea lor, se vor face electronic, prin intermediul platformei portal.caa.ro sau utilizând adresa de e-mail registratură@caa.ro.

Astfel, în urma evaluării manualului, AACR va formula eventualele neconformități în scris organizației. La primirea unor astfel de observații, organizația trebuie să revizuiască manualul, pentru a corecta neconformitățile. Pentru a avea o trasabilitate clară a modificărilor și pentru a permite evaluarea de către AACR a ISMM revizuit, organizația trebuie să răspundă în scris explicând modul în care au fost abordate neconformitățile și să revizuiască manualul ISMM identificând clar modificările introduse față de versiunea anterioară. Acest lucru se poate realiza prin:

- Menținerea manualului ISMM identificat drept „inițial” (adică ed.1, rev. 0), dar cu modificarea datei pentru noul proiect emis și
- Identificarea clară a textului modificat în fiecare capitol / paragraf ISMM (de exemplu, cu bare verticale sau evidențierea cu o culoare specifică a textului schimbat etc.)

Acest proces va fi continuat până când ISMM este considerat acceptabil de către AACR.

Notă: Același principiu se aplică reviziilor succesive ale ISMM și, de asemenea, documentelor asociate ISMM, cum ar fi procedurile și listele supuse aprobării AACR.

În capitolul destinat gestionării ISMM, organizația trebuie să menționeze modul în care prevede gestionarea schimbărilor ISMS având în vedere prevederile AMC1 IS.I/D.OR.255.

În cazul în care dorește utilizarea unei proceduri pentru gestionarea schimbărilor cu / fără aprobarea prealabilă a AACR, respectiva procedură trebuie descrisă astfel încât să satisfacă cel puțin cerințele AMC menționat mai sus.

Procedura se aprobă de către AACR odată cu aprobarea manualului.

2.4 Declarația Managerului Responsabil

Înainte de transmiterea ISMM spre aprobare la AACR, managerul responsabil trebuie să semneze declarația conținută în ISMM, confirmând astfel că a citit documentul și înțelege responsabilitățile ce îi revin. În cazul schimbării Managerului Responsabil, noul manager trebuie să semneze declarația și un amendament al manualului trebuie transmis spre aprobare la AACR.

Autoritatea Aeronautică Civilă Română

Referința		Ed./ rev. / data	
Denumirea organizației		Autorizare organizație nr.	

Secțiunea 3 EVALUARE CONȚINUT ISMM

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	PAGINA DE GARDĂ			
<input type="checkbox"/>	Manualul de management al securității informațiilor (ISMM)			
<input type="checkbox"/>	Codul documentului			
<input type="checkbox"/>	Numele oficial al organizației (conform cererii)			
<input type="checkbox"/>	Adresa, telefon, e-mail, fax al sediului social al organizației			
<input type="checkbox"/>	Referința aprobării/documente de certificare organizației			
<input type="checkbox"/>	Numărul exemplarului ISMM conform listei de distribuție			
<input type="checkbox"/>	Aprobarea internă a documentului (incluzând cel puțin numele în clar și semnăturile managerului Securitatea Informațiilor, monitorizarea conformării, managerului responsabil/CRP (Common Responsible Person)			
	PARTEA 0 – INTRODUCERE			
<input type="checkbox"/>	Introducere/ cuvânt înainte			
<input type="checkbox"/>	0.1 Cuprins	IS.I/D.OR.250		
<input type="checkbox"/>	0.2 Lista paginilor efective (LEP)	<i>NOTĂ: Lista paginilor efective (în vigoare) conținând ediția/ revizia fiecărei pagini a ISMM trebuie să permită trasabilitatea la versiunea anterior aprobată a ISMM. Se recomandă ca fiecare pagină a LEP să conțină aprobarea internă a manualului și referința aprobării indirecte, dacă este cazul.</i>		
<input type="checkbox"/>	0.3 Lista amendamentelor și Sumarul modificărilor	<i>NOTE: 1. Se recomandă ca pentru fiecare amendament (ediție/ revizie) să se indice secțiunile/ capitolele ISMM modificate și descrierea pe scurt a modificării efectuate la fiecărui capitol 2. Data efectivă a ediției /reviziei curente (reprezentând data la care amendamentul introdus intră în vigoare) trebuie menționată. În cazul aprobării inițiale și a modificărilor care necesită aprobare prealabilă a AACR aceasta nu poate fi anterioară datei aprobării ISMM de către AACR. 3. Procedurile care descriu modificările aduse sistemului de management al securității informației ISMS și ale manualului ISMM, cu sau fără aprobarea</i>		

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		<i>prealabilă a AACR, sunt descrise în capitolele 1.7 și 1.8.</i>		
<input type="checkbox"/>	0.4 Lista de distribuție <ul style="list-style-type: none"> ○ Nr. exemplarului ISMM ○ Deținător/ locație ○ Format (informatic, hârtie, etc.) 			
<input type="checkbox"/>	0.5 Abrevieri, terminologie și definiții	<i>GM1 IS.I/D.OR.200</i>		
<input type="checkbox"/>	0.6 Referințe încrucișate ISMM / manual integrat– cf. IS.I/D.OR.250 (d), dacă este aplicabil	<p><i>NOTĂ: Dacă organizația este autorizată ISO-IEC 27001:2022 sau NIS corelarea se va face cu punctele de reglementare din Appendix II din AMC & GM la Anexa II (Part-IS.I/D.OR) la regulamentul (EU) 2023/203 / (EU) 2022/1645 și EASA „Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS”.</i></p> <p><i>Dacă organizația descrie proceduri ISMS în alte manuale, atunci acest capitol va conține referința la manualul și capitolul aferent.</i></p>		
PARTEA 1 - MANAGEMENT				
<input type="checkbox"/>	1.1 Declarația Managerului Responsabil (Accountable Manager- AM) <ul style="list-style-type: none"> ○ se utilizează o declarație semnată de Managerul Responsabil (Accountable Manager), prin care se confirmă că organizația va desfășura, în orice moment, activitățile sale în conformitate cu prezenta Anexă și cu Manualul de Management al Securității Informației (ISMM). Orice modificare a declarației menționată mai sus nu trebuie să-i schimbe sensul. ○ Funcția, numele și semnătura AM. ○ Pentru și în numele organizației..... ○ Data ○ Dacă AM nu este directorul executiv CEO pentru organizație atunci CEO trebuie să contrasemneze declarația Organizația trebuie să demonstreze că managerul responsabil are acces direct la biroul directorului executiv și are alocate fondurile necesare pentru activitățile de securitatea informației preconizate. 1.1.1 Asigurarea accesului inspectorilor autorității competente <ul style="list-style-type: none"> ○ Angajamentul organizației de a acorda accesul la orice facilități/ aeronave/ componente, documente și înregistrări sau orice alte materiale relevante Part-IS. 1.1.2 Reacție imediată la probleme de siguranță	<i>IS.I/D.OR.250</i> <u>NOTE:</u> <i>1. De câte ori Managerul Responsabil este schimbat, noul Manager Responsabil trebuie să semneze declarația cât mai repede posibil, ca parte a procedurii de acceptare de către AACR.</i> <i>2. În scopul stabilirii conformării cu cerințele relevante ale Regulamentului (UE) 2023/203 și ale actelor sale delegate și de punere în aplicare.</i>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<ul style="list-style-type: none"> ○ Angajamentul organizației de a implementa măsurile de siguranță mandatate de către AACR precum și orice alte informații de siguranță obligatorii, relevante, emise de EASA inclusiv cele care decurg din incidente de securitate a informației și vulnerabilități care afectează siguranța. 			
☐	<p>1.2 Politica de Securitate și Obiective</p> <p>Politica de securitate a informațiilor trebuie să fie aprobată de Managerul Responsabil și revizuită la intervale planificate sau atunci când apar schimbări semnificative.</p> <p>Politica ar trebui să acopere cel puțin următoarele aspecte, care pot avea un potențial impact asupra siguranței aviației, prin care organizația se angajează să:</p> <ul style="list-style-type: none"> a) se conformeze cu toată legislația aplicabilă, să întrunească toate cerințele respecte legislația aplicabilă și să ia în considerare standardele și bunele practici relevante în domeniul securității informației; b) stabilească obiective și indicatori de performanță pentru gestionarea securității informației; c) definească principii generale, activități și procese prin care organizația să asigure în mod corespunzător securitatea sistemelor și tehnologiilor informaționale și a datelor, inclusiv stabilirea unei scheme de clasificare a informațiilor în funcție de nivelul de sensibilitate al acestora, fie că sunt utilizate, generate sau primite de la alte părți; d) integreze cerințele ISMS în procesele organizației; e) urmărească îmbunătățirea continuă către niveluri superioare de maturitate a proceselor de securitate a informației, conform IS.I/D.OR.260; f) respecte cerințele aplicabile privind securitatea informației și managementul său proactiv și sistematic, precum și să asigure resursele adecvate pentru implementare și funcționare; g) atribuie securitatea informației ca una dintre responsabilitățile esențiale ale tuturor managerilor; h) promoveze Politica de Securitate a Informației prin instruirii sau sesiuni de conștientizare în cadrul organizației, adresate întregului personal, în mod regulat sau ori de câte ori intervin modificări; i) încurajeze implementarea unei „culturi juste” (just culture) și raportarea vulnerabilităților, a evenimentelor suspecte/anormale și/sau a incidentelor de securitate a informației; j) comunice Politica de Securitate a Informației tuturor părților relevante, după caz; 	<p><i>IS.I/D.OR.200(a)(1), AMC1 IS.I/D.OR.200(a)(1), GM1 IS.I/D.OR.200(a)(1), IS.I/D.OR.250(a)(4); GM1 IS.I/D.OR.200(c)</i></p> <p><u>NOTE:</u></p> <p><i>1. Politica de Securitate a Informației și obiectivele aferente trebuie să aibă ca element central conceptul de siguranță a aviației și să fie adecvate nivelului de complexitate, în ceea ce privește securitatea informației, al organizației. Această complexitate este determinată de următoarele elemente:</i></p> <ul style="list-style-type: none"> • <i>Poziția organizației în lanțul funcțional și numărul, precum și relevanța pentru siguranță, a organizațiilor/părților interesate cu care interacționează.</i> • <i>Complexitatea structurii organizaționale și a ierarhiilor (de ex. numărul de angajați, departamente, niveluri ierarhice, locații externe, filiale etc.).</i> <p><i>Complexitatea sistemelor și datelor IT&C utilizate de organizație și conexiunile acestora cu părți externe.</i></p> <p><i>Ghidul privind elementele care influențează complexitatea organizației poate fi consultat în Anexa V la AMC & GM la Partea IS.I/D.OR – Considerații de proporționalitate legate de indicatorii de complexitate.</i></p> <p><i>2. Angajamentul de a aplica principiile „culturii juste” formează baza regulilor interne ale organizației, care descriu modul în care sunt garantate și implementate principiile „culturii juste”.</i></p> <p><i>3. Exemple tipice (neexhaustive) de indicatori-cheie de performanță (KPIs), care pot fi stabiliți (dacă sunt</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>k) se asigure că fiecare acțiune întreprinsă în baza acestei Politici de Securitate a Informației este orientată către îmbunătățirea siguranței aviației;</p> <p>l) revizuiască și, dacă este necesar, să modifice Politica de Securitate a Informației ori de câte ori activitățile și/sau complexitatea organizației se schimbă sau dacă organizația constată că această politică nu este eficientă.</p> <p>Organizația trebuie, de asemenea, să includă o listă de obiective și indicatori-cheie de performanță privind securitatea informației. Obiectivele trebuie să fie:</p> <ul style="list-style-type: none"> • Consistente și aliniate cu Politica de Securitate a Informației. • Măsurabile, pentru a permite stabilirea gradului de îndeplinire a obiectivelor. • Revizuite periodic, pentru a asigura actualitatea și adecvarea lor. 	<p>corelați cu obiectivele stabilite de organizație) sunt următoarele:</p> <p><i>Evaluarea și tratarea riscurilor:</i></p> <ul style="list-style-type: none"> • <i>Numărul de riscuri identificate: monitorizarea variațiilor în numărul de riscuri identificate pe parcursul evaluărilor.</i> • <i>Timpul de atenuare a riscurilor: durata medie necesară pentru implementarea măsurilor de tratare a riscurilor.</i> <p><i>Politici și proceduri:</i></p> <ul style="list-style-type: none"> • <i>Rata de conformare cu politicile: procentul angajaților care respectă politicile de securitate, pe baza rezultatelor auditurilor.</i> • <i>Numărul de neconformități: probleme de nerespectare identificate în cadrul auditurilor interne/externe.</i> <p><i>Controale de securitate (măsuri):</i></p> <ul style="list-style-type: none"> • <i>Încălcări ale controlului accesului: numărul de tentative sau accesări neautorizate detectate.</i> • <i>Acoperirea revizuirii jurnalelor: procentul jurnalelor de securitate analizate într-un interval de timp definit.</i> <p><i>Managementul incidentelor:</i></p> <ul style="list-style-type: none"> • <i>Timpul de rezolvare a incidentelor: durata medie necesară pentru soluționarea incidentelor raportate.</i> • <i>Timpul de indisponibilitate cauzat de incidente de securitate: durata totală de nefuncționare a sistemelor critice pentru siguranță.</i> <p><i>Instruirea și conștientizarea:</i></p> <ul style="list-style-type: none"> • <i>Rata de finalizare a instruirii: procentul angajaților care finalizează instruirea privind securitatea informației.</i> • <i>Rata de succes la simulările de phishing: numărul angajaților care identifică corect tentativele de phishing.</i> 		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
<input type="checkbox"/>	<p>1.3 Monitorizarea conformării</p> <p>Organizația trebuie să implementeze o funcție de monitorizare periodică a conformării sistemului de management cu cerințele relevante și a adecvării procedurilor, inclusiv prin instituirea unui proces intern de audit și a unui proces de gestionare a riscurilor de securitate a informațiilor.</p> <p>Monitorizarea conformării trebuie să includă un mecanism de feedback privind constatările auditului către persoana responsabilă.</p> <p>Auditurile interne trebuie desfășurate la intervale planificate pentru a oferi garanții privind starea ISMS către conducere și pentru a furniza informații referitoare la următoarele aspecte:</p> <ul style="list-style-type: none"> – conformarea ISMS cu cerințele prezentului regulament și cu cerințele proprii ale organizației, fie stabilite în politica de securitate a informațiilor, proceduri și contracte, fie derivate din obiectivele de securitate a informațiilor sau din rezultatele procesului de tratare a riscurilor; – implementarea și menținerea eficientă a ISMS. 	<p><i>IS.1/D.OR.200(a)(12), AMC1 IS.1/D.OR.200(a)(12), GM1 IS.1/D.OR.200(a)(12)</i></p> <p><i>Auditurile interne trebuie să urmeze o abordare independentă și un proces decizional bazat pe dovezi.</i></p> <p><i>La stabilirea unui program de audit, trebuie luate în considerare importanța proceselor vizate, precum și definirea criteriilor și a domeniului auditului.</i></p> <p><i>Trebuie păstrate informații documentate care să ateste rezultatele auditului, raportarea acestora către conducerea relevantă, precum și programul de audit.</i></p>		
<input type="checkbox"/>	<p>1.4 Personalul de Conducere</p> <ul style="list-style-type: none"> <input type="checkbox"/> Manager Responsabil <input type="checkbox"/> Persoană cu Responsabilitate Comună- CRP (common responsible person), dacă este cazul. <input type="checkbox"/> Manager /Responsabil securitate informațiilor - nominalizat conform prevederilor PART IS.1/D.OR.240(b) <input type="checkbox"/> Manager monitorizare conformare (inclusiv pentru cerințele Partea-IS) al organizației; 	<p><i>IS.1/D.OR.240(b), IS.1/D.OR.240(c), IS.1/D.OR.240(d), IS.1/D.OR.250(a)(2), IS.1/D.OR.250(a)(3), IS.1/D.OR.250(a)(6)</i></p> <p>NOTE:</p> <p>1. Capitolul trebuie să identifice structura managementului, listând cel puțin numele și funcțiile managerului responsabil și a personalului nominalizat în funcțiile de conducere specificate în PART IS. De asemenea trebuie identificați și înlocuitorii. Personalul nominalizat trebuie să acopere prin responsabilitățile definite, toate funcțiile PART IS aplicabile. Organizația poate adopta orice denumire pentru funcțiile manageriale, cu condiția să identifice denumirile și persoanele alese să îndeplinească aceste funcții.</p> <p>In cazul in care aceeași persoană este nominalizată să gestioneze mai multe funcții, managerul responsabil trebuie să se asigure că sunt alocate resurse suficiente ambelor funcții, ținând cont de</p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		<p>dimensiunea organizației, precum și de natura și complexitatea activităților.</p> <p>2.În ceea ce privește securitatea informației și, în funcție de nivelul de complexitate al organizației, aceasta poate introduce funcții suplimentare, cum ar fi:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Manager risc securitatea informațiilor <input type="checkbox"/> Manager raportare securitate informațională <input type="checkbox"/> Responsabil răspuns la incidente de securitate informațională <input type="checkbox"/> Responsabil cu implementarea soluțiilor de securitate a informațiilor (pentru soluții de securitate a informațiilor) <input type="checkbox"/> Specialist informații despre amenințări (Threat Intelligence Specialist) <input type="checkbox"/> Arhitect securitate informațională <input type="checkbox"/> Instructor/educator securitate informațională <input type="checkbox"/> Investigator în criminalistică digitală (Digital Forensic Investigator) <input type="checkbox"/> Analist în testarea vulnerabilităților (Penetration tester) <p>Aceste persoane trebuie, în final, să raporteze persoanelor nominalizate pentru Part-IS (de ex. Manager securitate informațiilor, Manager tehnologia informației).</p> <p>3.Alți posibili manageri sunt la latitudinea organizației.</p> <p>Listă posibili manageri:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Manager audit; <p>Manager tehnologia informației (dacă această persoană nu raportează Managerului securitatea informațiilor și este responsabilă de anumite sarcini din Partea-IS, atunci aceasta trebuie să fie, de asemenea, una dintre persoanele nominalizate)</p>		
<input type="checkbox"/>	1.5 Sarcinile și Responsabilitățile Personalului de Conducere Cerințe privind personalul	<p><i>IS.I/D.OR.200(a)(10);IS.I/D.OR.200(c), AMC1</i></p> <p><i>IS.I/D.OR.200(c), GM1 IS.I/D.OR.200(c);</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>Acest capitol trebuie să descrie următoarele:</p> <p>(a) Cerințele de calificare aplicabile personalului implicat în activitățile din cadrul Part-IS, astfel încât organizația să se asigure că aceștia dețin competențele necesare pentru îndeplinirea sarcinilor.</p> <p>(b) Procesul implementat pentru a se asigura că personalul înțelege și confirmă responsabilitățile asociate rolurilor și sarcinilor atribuite.</p> <p>(c) O clasificare predefinită a nivelurilor de încredere necesare personalului pentru a avea acces la diferitele sisteme informatice și date utilizate de organizație, în funcție de gravitatea consecințelor asupra siguranței, identificate prin evaluarea de risc aplicabilă.</p> <p>(d) Procedura utilizată pentru verificarea identității și evaluarea nivelului de încredere al personalului menționat la punctul (c) de mai sus. (Indicații suplimentare pot fi găsite în GM1 IS.I/D.OR.240(i).)</p> <p>(e) Dovezi ale competențelor actuale ale personalului care desfășoară activitățile prevăzute de Part-IS</p> <p>ISMM capitolul 1.5 trebuie să fie în concordanță cu ISMM capitolele 1.4 și 1.6 și să prezinte descrierea actualizată a structurii managementului organizației.</p> <p>1.5.1 Manager Responsabil (MR)</p> <ul style="list-style-type: none"> ○ stabilirea și promovarea politicilor de siguranță și de securitate a informațiilor; ○ numirea personalului de conducere cu responsabilități în Part IS; ○ asigurarea faptului că sunt disponibile resursele financiare, umane și facilitățile necesare pentru implementarea și menținerea ISMS ○ asigurarea faptului că a fost evaluată competența întregului personal, inclusiv a personalului de conducere implicat în ISMS; <p><u>NOTĂ:</u> Responsabilitățile indicate acoperă aspectele Part-IS. În cazul în care organizația își partajează structurile organizaționale de securitate a informațiilor, politicile, procesele și procedurile cu alte organizații sau cu alte departamente din cadrul propriei organizații care nu fac parte din aprobare sau declarație, Managerul Responsabil poate, opțional, să delege activitățile legate de securitatea informațiilor unei „Persoane cu Responsabilitate Comună” (Common Responsible Person – CRP), în conformitate cu articolele IS.I/D.OR.240(d) și (e).</p> <p>Această persoană trebuie să dețină autoritate la nivel înalt în cadrul corporației, precum și competențele și autoritatea necesare pentru a lua deciziile corespunzătoare și pentru a controla și mobiliza resursele și mijloacele financiare necesare între diferitele organizații.</p>	<p>IS.I/D.OR.240; GM1 IS.I/D.OR.240; AMC1 IS.I/D.OR.240(a)(2); AMC1 IS.I/D.OR.240(a)(3); GM1 IS.I/D.OR.240(a)(3); IS.I/D.OR.240(b), AMC1 IS.I/D.OR.240(b); GM1 IS.I/D.OR.240(b); GM1 IS.I/D.OR.240(b)&(c); IS.I/D.OR.240(c), GM1 IS.I/D.OR.240(c); IS.I/D.OR.240(d), AMC1 IS.I/D.OR.240(d); IS.I/D.OR.240(e), GM1 IS.I/D.OR.240(e); AMC1 IS.I/D.OR.240(f); GM1 IS.I/D.OR.240(f); AMC1 IS.I/D.OR.240(g); GM1 IS.I/D.OR.240(g); AMC1 IS.I/D.OR.240(h); GM1 IS.I/D.OR.240(h); AMC1 IS.I/D.OR.240(i); GM1 IS.I/D.OR.240(i) IS.I/D.OR.250(a)(2), IS.I/D.OR.250(a)(3), IS.I/D.OR.250(a)(6), IS.I/D.OR.250(a)(7)</p> <p><i>Orice funcție Part-IS aplicabilă organizației trebuie să fie în responsabilitatea unui manager nominalizat listat în cap. 1.4</i></p> <p><u>NOTE:</u></p> <p>1) Sarcinile (atribuțiile) oricărei Persoane nominalizate pot fi delegate către alți manageri care îi sunt subordonați</p> <p>2) sistemul de monitorizarea conformării este necesar să fie "independent", ceea ce înseamnă în mod normal că Managerul Monitorizarea Conformării și auditorii nu sunt direct implicați în activitățile Part IS care urmează să fie auditate</p> <p>3) Următoarele cerințe privind personalul pot fi acoperite în alte părți ale prezentului ISMM, după cum se detaliază mai jos:</p> <ul style="list-style-type: none"> ○ Personalul de conducere, atribuțiile și responsabilitățile acestuia, ○ precum și organigrama de management (ref. IS.I/D.OR.200(c), IS.I/D.OR.240(a)-(e), IS.I/D.OR.250(a)(2), (a)(3), (a)(6) și (a)(7)) ○ Cerințele de calificare pentru personalul de monitorizare a conformării (ref. IS.I/D.OR.240(g)) 		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>Această delegare de activități nu implică o delegare a responsabilității, care rămâne în continuare la Managerul Responsabil.</p> <p>În consecință, trebuie stabilită o coordonare adecvată între Managerul Responsabil și Persoana cu Responsabilitate Comună , pentru a se asigura că politicile și deciziile luate la nivel corporativ (de către Persoana cu Responsabilitate Comună) continuă să corespundă nevoilor organizației aprobate.</p> <p>1.5.2 Managerul pentru monitorizarea conformării</p> <p>Este responsabil pentru <i>monitorizarea conformării cu PART IS.</i></p> <p><i>Responsabilități:</i></p> <ul style="list-style-type: none"> • asigurarea faptului că activitățile ISMS sunt monitorizate pentru conformarea cu cerințele aplicabile și cu orice cerințe suplimentare stabilite de organizație, precum și pentru a se asigura că aceste activități sunt efectuate în mod corespunzător, sub supravegherea persoanelor nominalizate; • asigurarea faptului că orice activitate contractată unei alte organizații este monitorizată din punct de vedere ISMS pentru conformarea cu contractul sau comanda de lucru; • stabilirea unui sistem independent de audit pentru monitorizarea conformării organizației cu cerințele regulamentelor (EU) 2023/203 și/sau (EU) 2022/1645, precum și pentru a se asigura că planul de audit este implementat corespunzător, menținut și revizuit continuu pentru îmbunătățire; • solicitarea corecțiilor și acțiunilor corective atunci când este necesar; • organizarea de întâlniri periodice cu Managerul Responsabil, pentru evaluarea eficacității sistemului de Monitorizare a Conformării; aceste întâlniri vor include detalii despre orice neconformitate raportată care nu a fost abordată corespunzător de persoana responsabilă sau despre eventuale neînțelegeri privind natura unei neconformități; • monitorizarea actualizării procedurilor și practicilor standard ale organizației și verificarea conformării acestora cu ultima revizie a Regulamentelor (EU) 2023/203 și/sau (EU) 2022/1645, precum și cu orice alte cerințe sau materiale de ghidare emise de EASA; • transmiterea manualului ISMM și a oricăror amendamente asociate către autoritatea competentă pentru aprobare (inclusiv completarea și transmiterea cererii de modificare/ autorizare); 	<p><i>Evaluarea competenței personalului (ref. IS.I/D.OR.240(g)</i></p> <p><i>4) Exemple de activități de management al securității informațiilor care pot fi externalizate / contractate se găsesc în Tabel 1 din GM3 IS.I/D.OR.235.</i></p> <p><i>5) În cazul în care același personal îndeplinește atât atribuții Part-IS, cât și responsabilități în cadrul SMS, calificările și competențele acestuia trebuie să fie corelate și conforme cu cerințele aplicabile din SMS, pentru a asigura o abordare integrată și coerentă a proceselor organizației.</i></p> <p><i>6) Orice funcție Part-IS care este aplicabilă Organizației trebuie să se afle sub responsabilitatea unei Persoane nominalizată, așa cum este listată în capitolul 1.4, care trebuie să asigure conformarea acelei funcții cu cerințele relevante din reglementări.</i></p> <p><i>Responsabilitățile unei Persoane Nominalizate nu pot fi delegate altor manageri, cu excepția cazului în care aceștia sunt identificați drept „Manager Adjunct Nominalizat” (Deputy Nominated Person) pentru funcția respectivă (de exemplu: Adjunct al Managerului de securitatea informațiilor).</i></p> <p><i>Atribuțiile oricărei Persoane Nominalizate pot fi delegate altor manageri care se află sub coordonarea sa (care îi raportează direct).</i></p> <p><i>7) Managerii organizației pot fi nominalizați și pentru rolurile prevăzute de Part-IS, cu condiția respectării competențelor și nivelului de autoritate cerut de reglementările în vigoare.</i></p> <p><i>Managerii organizației pot fi nominalizați și pentru rolurile prevăzute de Part-IS, exercitând responsabilități comune în limitele competențelor și autorității stabilite de reglementările în vigoare. Atribuțiile acestora trebuie corelate și reflectate în manualele relevante ale organizației (ex.: CAME,</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<ul style="list-style-type: none"> • evaluarea furnizorilor și a organizațiilor contractate pentru activități ISMS, pentru a se asigura de calitatea satisfăcătoare a produselor/ serviciilor, în raport cu nevoile organizației; • integrarea rezultatelor auditurilor și a constatărilor aferente în programul de instruire recurentă al organizației. <p>Poate delega atribuții către managerii din subordine, de ex: Managerul pentru Audit, dacă se aplică.</p> <p>1.5.3 Managerul de siguranță Managerul de Siguranță oferă suport Managerului de Securitatea Informațiilor (Information Security Manager) în stabilirea legăturilor adecvate între siguranță și securitatea informațiilor și, în special, în identificarea și evaluarea impactului asupra siguranței pe care îl pot avea riscurile, evenimentele, incidentele sau vulnerabilitățile de securitate a informațiilor.</p> <p>1.5.4 Managerul de Securitatea Informațiilor (Information Security Manager) Managerul de Securitatea Informațiilor raportează direct Managerului Responsabil (Accountable Manager)/ CRP și este responsabil pentru dezvoltarea, administrarea și menținerea proceselor de management al securității informațiilor din cadrul organizației.</p> <ul style="list-style-type: none"> ○ Definirea, implementarea, comunicarea și menținerea obiectivelor, cerințelor, strategiilor și politicilor de securitate a informațiilor, ținând cont de integrarea perspectivei de siguranță (safety). ○ Aceasta trebuie să asigure că măsurile de securitate a informațiilor nu compromit siguranța sistemelor și proceselor operaționale. Considerațiile legate de siguranță trebuie incluse în evaluările de risc, modelele de amenințări și procesele decizionale; ○ Pregătirea și prezentarea viziunii, strategiilor și politicilor privind securitatea informațiilor spre aprobare conducerii superioare a organizației și asigurarea implementării acestora, subliniind implicațiile asupra siguranței și importanța alinierii măsurilor de securitate la obiectivele de siguranță operațională. ○ Scopul este ca managementul superior să înțeleagă impactul potențial al deciziilor privind securitatea informațiilor asupra siguranței generale a organizației; 	<p><i>MOE, SMS, ISMM, etc.), pentru a asigura coerența și conformitatea structurii de management.</i></p> <p><i>8) Evenimentele de aviație cu relevanță pentru siguranța operațională se raportează în platforma ECCAIRS, sub responsabilitatea persoanei nominalizate în structura de management (ex.: Safety Manager / Compliance Manager).</i></p> <p><i>Incidentele de securitate cibernetică se raportează la DNSC prin PNRISC, de către Managerul securitatea informațiilor (ex.: IT Security Manager / Responsabil Part-IS).</i></p> <p><i>În situațiile în care un incident prezintă implicații atât asupra siguranței operaționale, cât și asupra securității cibernetice, responsabilitățile sunt exercitate în mod comun, cu obligația coordonării între managerii responsabili și cu completarea ambelor fluxuri de raportare.</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<ul style="list-style-type: none"> ○ Supravegherea aplicării și îmbunătățirii Sistemului de Management al Securității Informațiilor (ISMS), cu accent pe componenta de siguranță, în coordonare cu Managerul de Siguranță (Safety Manager). ○ În exercitarea acestei funcții, accentul trebuie pus pe supravegherea controalelor introduse în cadrul ISMS pentru a se asigura că cerințele de siguranță sunt îndeplinite și pe monitorizarea eficienței măsurilor de siguranță implementate împreună cu practicile de securitate a informațiilor; ○ Instruirea managementului superior în ceea ce privește riscurile și amenințările la adresa securității informațiilor, precum și impactul acestora asupra organizației și a organizațiilor cu care aceasta interacționează, având permanent în vedere perspectiva siguranței. ○ Acest proces trebuie să permită conducerii să înțeleagă consecințele potențiale ale incidentelor de securitate asupra siguranței operaționale și să poată lua decizii informate privind alocarea resurselor și strategiile de reducere a riscurilor; ○ Asigurarea aprobării, de către managementul superior, a riscurilor de securitate a informațiilor ale organizației, ținând cont de aspectele de siguranță și tratând implicațiile asupra siguranței asociate acestor riscuri; <p>Elaborarea planurilor de securitate a informațiilor care integrează considerentele de siguranță, concentrându-se nu doar pe protecția împotriva amenințărilor cibernetice, ci și pe includerea măsurilor legate de siguranța operațională. Acestea pot include introducerea controalelor de siguranță, efectuarea de evaluări ale impactului asupra siguranței și alinierea inițiativelor de securitate cibernetică cu obiectivele de siguranță și standardele specifice industriei;</p> <ul style="list-style-type: none"> ○ Dezvoltarea relațiilor de colaborare cu autoritățile și comunitățile specializate în domeniul securității cibernetice, cu accent pe aspectele legate de siguranță; ○ Raportarea incidentelor, riscurilor și constatărilor privind securitatea informațiilor către managementul superior, evidențiind orice implicații asupra siguranței; ○ Evaluează incidentul pentru a determina dacă se califică drept „incident de securitate cibernetică cu impact semnificativ” conform PNRISC și raportează către DNSC în termen de 24 ore conform cerințelor aplicabile. <ul style="list-style-type: none"> ○ Actualizează analiza de risc Part-IS/ISMS după incident. ○ Monitorizarea evoluțiilor în domeniul securității informațiilor, cu accent pe tehnologiile și practicile legate de siguranță; 			

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<ul style="list-style-type: none"> ○ Negocierea bugetului de securitate a informațiilor cu managementul superior; ○ Asigurarea rezilienței organizației în fața incidentelor de securitate a informațiilor, prin integrarea unor planuri de răspuns la incidente și măsuri de continuitate a activității orientate spre siguranță. Aceasta implică identificarea și tratarea riscurilor potențiale pentru siguranță în timpul proceselor de răspuns la incidente și de recuperare; ○ Gestionarea procesului de dezvoltare continuă a capacităților interne în cadrul organizației, prin promovarea programelor de instruire și conștientizare care să includă atât aspectele de securitate a informațiilor, cât și pe cele de siguranță operațională; ○ Revizuirea, planificarea și alocarea resurselor adecvate pentru securitatea informațiilor, ținând cont de cerințele de siguranță și efectuând evaluări periodice ale necesarului de resurse, pentru a asigura protecția eficientă a sistemelor și menținerea siguranței operaționale. <p>1.5.6 Managerul Tehnologiei Informației (Information Technology – IT Manager), dacă se aplică organizației</p> <p>Dacă o parte dintre activitățile cerute de Part-IS sunt îndeplinite de Managerul IT (Information Technology Manager), pot apărea două situații diferite:</p> <ul style="list-style-type: none"> • Cazul în care Managerul IT raportează Managerului securitatea informațiilor (Information Security Manager): În această situație, activitățile Part-IS îndeplinite de Managerul IT (de exemplu: definirea arhitecturii IT, detectarea evenimentelor/incidentele, răspunsul la incidente, investigațiile criminalistice digitale etc.) sunt realizate prin delegare de la Managerul Securitatea Informațiilor, care rămâne responsabil pentru acestea; • Cazul în care Managerul IT nu raportează Managerului securitatea informațiilor: În această situație, Managerul IT trebuie să fie, de asemenea, una dintre persoanele nominalizate (nominated persons), fiind astfel direct responsabil pentru activitățile respective. 			

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
☐	<p>1.6 Organigrama managementului organizației</p> <p>Organizația trebuie să:</p> <p>(a) furnizeze o organigramă a structurii personalului dedicat securității informațiilor (intern și extern), inclusiv rolurile și responsabilitățile acestora. Această organigramă a structurii trebuie să fie integrată în organigrama generală a organizației, așa cum este definită în manualul de prezentare specific fiecărei autorizări și va fi utilizată pentru a gestiona și menține elementele incluse în domeniul de aplicare al ISMS și va fi aprobată de managerul responsabil. Organizația trebuie să revizuiască organigrama structurii la intervale planificate sau în cazul în care au loc modificări semnificative (a se vedea nota din AMC1 IS.1/D.OR.200(a)(1)).</p> <p>Organigramă trebuie să ilustreze legăturile funcționale dintre Managerul responsabil, persoanele responsabile de implementarea și managementul ISMS, și de funcția de monitorizare a conformării.</p> <ul style="list-style-type: none"> ○ Personalul nominalizat în funcții de conducere (trebuie acceptat de AACR) trebuie să fie indicat în organigramă. Numele personalului de conducere poate să fie menționat în organigramă, dar nu este obligatoriu. ○ Personalul nominalizat în funcții de conducere trebuie să aibă acces direct la managerului responsabil/ CRP (<i>Common Responsible Person</i>). 	<p><i>IS.1/D.OR.200(c); AMC1 IS.1/D.OR.200(c); GM1 IS.1/D.OR.200(c); IS.1/D.OR.250(a)(7)</i></p> <p>NOTE:</p> <p><i>1) Există diferite moduri de a configura structura organizatorică. Principiul cheie este că, indiferent de aranjament, există o persoană nominalizată responsabilă pentru fiecare funcție Part-IS și această responsabilitate este recunoscută prin persoana nominalizată și managerul responsabil. Această responsabilitate nu trebuie diluată în diferitele niveluri de management și trebuie să nu existe conflicte de interese</i></p> <p><i>2. Personalul de monitorizare a conformării (ex: auditorul calității) trebuie să demonstreze că este independent de managerii de Part-IS.</i></p> <p><i>3. În cazul în care organizația deține mai multe autorizări și/sau gestionează aspecte privind securitatea informațiilor cu alte organizații sau cu zone din propria organizație nesupuse autorizării, Managerul Responsabil poate, ca opțiune, delega activitățile legate de securitatea informațiilor către o „Persoană cu Responsabilitate Comună ” (CRP – Common Responsible Person), în conformitate cu IS.1/D.OR.240(d) și (e).</i></p> <p><i>Această persoană trebuie să dețină autoritate la un nivel înalt în cadrul organizației (corporate level), precum și competența și autoritatea necesare pentru a lua decizii corespunzătoare, pentru a controla și mobiliza resursele financiare și materiale necesare în cadrul diferitelor organizații.</i></p> <p><i>Această delegare a activităților nu implică delegarea responsabilităților, care rămân în continuare în sarcina Managerului Responsabil.</i></p> <p><i>Ca urmare, trebuie stabilită o coordonare adecvată între Managerul Responsabil și Persoana Responsabilitate Comună , pentru a se asigura că politicile și deciziile luate la nivel corporativ (de către</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		Persoana Responsabilitate Comună) răspund în continuare nevoilor organizației aprobate.		
<input type="checkbox"/>	<p>1.6 Resurse de manoperă</p> <ul style="list-style-type: none"> ○ Organizația trebuie să poată demonstra că dispune de resurse de personal adecvate pentru a susține activitatea specifică Part-IS. ○ Organizația nu trebuie să declare un procent al personalului utilizat, ci să indice numărul de angajați necesar pentru a se conforma cerințelor Part-IS. ○ Defalcarea numărului total de personal pe diferitele categorii de personal. Se așteaptă un tabel rezumativ cu personal pentru managementul securității informațiilor. ○ Se recomandă ca numărul de angajați alocat domeniului Part-IS să fie corelat cu necesarul estimat de MH pentru organizație, pentru a demonstra adecvarea resurselor și pentru a susține o planificare coerentă a activităților. 	IS.I/D.OR.240(f), AMC1 IS.I/D.OR.240(f), GM1 IS.I/D.OR.240(f), IS.I/D.OR.250(a)(5)		
<input type="checkbox"/>	<p>1.7 Proceduri pentru modificări ale ISMS, inclusiv ISMM care necesită aprobare prealabilă</p> <p>Acest capitol trebuie să descrie modificările ISMS/ ISMM care necesită aprobarea prealabilă a AACR.</p> <p>1.7.1. Lista modificărilor și proceduri de notificare AACR</p> <p>NOTĂ: Lista modificărilor cu impact asupra ISMS (conform AMC1 IS.I./D.OR.255 și GM2 IS.I./D.OR.255) poate fi realizată într-un tabel conținând tipul modificării și documentele necesar a fi transmise la AACR. Este acceptabilă includerea procedurii de modificare a ISMS în procedura deja existentă din manualul de prezentare al organizației, specific fiecărei autorizări/ manual de management integrat, etc.</p> <p>1.7.2. Descrierea procesului de aprobare internă.</p> <p>1.7.3. Proceduri de amendare a manualului ISMM.</p> <p>1.7.4. Trasmiterea solicitării de modificare către AACR.</p>	<p>IS.I./D.OR.250(b)(c), GM1 IS.I./D.OR. 250 (a)</p> <p>AMC1 IS.I/D.OR.255, GM1 IS.I/D.OR.255 și GM2 IS.I/D.OR.255</p> <p><u>NOTE:</u></p> <p>1)Organizația va ține cont de procedurile existente din manualele aplicabile, inclusiv cele privind gestionarea modificărilor (MOC), evaluarea riscurilor și măsurile de mitigare, asigurând utilizarea unui set comun de procese chiar dacă vor exista manuale distincte. În acest mod se menține coerența și trasabilitatea activităților, fără a introduce un program suplimentar de monitorizare a conformării pentru Part-IS , utilizând în schimb procedurile unificate și mecanismele interne deja stabilite pentru monitorizare și control.</p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		2) Orice schimbare sau modificare a proceselor necesită cel puțin un Management of Change, iar, după caz, efectuarea unui audit de evaluare pentru a verifica impactul, conformitatea și eficacitatea modificării.		
☐	<p>1.8 Proceduri pentru modificări ale ISMS, inclusiv ISMM care nu necesită aprobare prealabilă</p> <p>Acest capitol trebuie să descrie modificările ISMS/ISMM care nu necesită aprobarea prealabilă a AACR.</p> <p>1.8.1. Definirea modificărilor care nu au impact asupra ISMM</p> <p>NOTĂ: Lista modificărilor fără impact asupra ISMS (conform GM2 IS.1./D.OR.255 poate fi realizată într-un tabel conținând tipul modificării și documentele necesar a fi transmise la AACR. Este acceptabilă includerea acestei proceduri în procedura deja existentă din manualul de prezentare al organizației, specific fiecărei autorizări/ manual de management integrat, etc.</p> <p>1.8.2. Descrierea procesului de aprobare internă.</p> <p>1.8.3. Proceduri de amendare a manualului ISMM.</p> <p>1.8.4. Notificarea AACR cu privire la modificările care nu necesită aprobare prealabilă.</p>	<p>IS.1./D.OR.250(b)(c), GM1 IS.1./D.OR. 250 (a) AMC1 IS.1/D.OR.255, GM1 IS.1/D.OR.255 și GM2 IS.1/D.OR.255 GM2 IS.1/D.OR.255</p> <p><u>NOTE:</u></p> <p>1)Orice schimbare sau modificare a proceselor necesită cel puțin un Management of Change, iar, după caz, efectuarea unui audit de evaluare pentru a verifica impactul, conformitatea și eficacitatea modificării.</p> <p>2)Exemple de modificări care nu au impact asupra ISMS, ar fi următoarele:</p> <ul style="list-style-type: none"> • După detectarea cu succes a unui eveniment de securitate a informațiilor care ar fi putut evolua cu ușurință într-un incident, organizația decide să implementeze o sesiune extinsă de conștientizare în domeniul securității cibernetice pentru toți angajații. • Actualizarea programului de instruire a personalului și/sau a conținutului instruirii ca rezultat al proceselor de îmbunătățire continuă stabilite în cadrul organizației. • Organizația înlocuiește instrumentul software utilizat pentru criptarea fișierelor sensibile cu o altă soluție software. • Organizația decide să efectueze o restructurare internă din motive comerciale, schimbând denumirile departamentelor sau secțiunilor, fără a aduce modificări responsabilităților sau atribuțiilor (de exemplu, ale managerului responsabil) care implică ISMS-ul organizației. 		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		<ul style="list-style-type: none"> Organizația decide să actualizeze un control preventiv existent, de exemplu prin configurarea unui nou firewall în rețeaua sa internă. 		
☐	<p>2.1 Evaluarea Riscurilor de Securitate a Informațiilor</p> <p>2.1.1. Scopul acestei proceduri este de a stabili o inventariere completă a tuturor activelor, resurselor și dependențelor relevante care fac parte în mod direct din funcțiile, serviciile și capacitățile organizației, prin desfășurarea următoarelor activități:</p> <p>(a) Identificarea intrărilor și ieșirilor operaționale relevante pentru funcțiile, serviciile și capacitățile organizației; acestea pot fi asociate cu:</p> <ul style="list-style-type: none"> – surse interne sau externe; – servicii interne sau externe închiriate ori gestionate, sau alte dependențe; <p>(b) Identificarea tuturor activelor relevante (de exemplu: echipamente hardware, aplicații software, resurse de rețea și de calcul) utilizate pentru a crea, procesa, transmite, stoca sau primi intrările și ieșirile operaționale menționate anterior;</p> <p>(c) Identificarea mediilor operaționale (de exemplu: birouri, zone cu acces public, camere cu acces controlat etc.) și a locațiilor tuturor activelor relevante;</p> <p>(d) Pentru fiecare activ și mediu operațional inclus în domeniul de aplicare, identificarea metodelor, proceselor și resurselor specifice care vor fi utilizate pentru accesul, gestionarea, operarea și întreținerea acestuia pe parcursul întregului său ciclu de viață, inclusiv:</p> <ul style="list-style-type: none"> – resurse interne sau contractate; – companii contractate care gestionează de la distanță activele (de exemplu, furnizorii de servicii gestionate). <p>2.1.2. Acest capitol trebuie să descrie următoarele:</p> <p>(a) Procedura utilizată pentru identificarea elementelor organizației care ar putea fi expuse riscurilor privind securitatea informațiilor, incluzând:</p> <ol style="list-style-type: none"> (1) activitățile, facilitățile și resursele organizației, precum și serviciile pe care organizația le operează, le furnizează, le primește sau le întreține; (2) echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor menționate la punctul (1) de mai sus. <p>Procedura trebuie, de asemenea, să specifice metoda utilizată de organizație pentru a înregistra elementele care ar putea fi expuse riscurilor privind securitatea informațiilor (de exemplu, printr-un șablon predefinit pentru un inventar al activelor).</p>	<p><i>IS.I/D.OR.200(a)(2) ; IS.I/D.OR.205, GM1 IS.I/D.OR.205, AMC1 IS.I/D.OR.205(a), GM1 IS.I/D.OR.205(a), AMC1 IS.I/D.OR.205(b), GM1 IS.I/D.OR.205(b), GM2 IS.I/D.OR.205(b), AMC1 IS.I/D.OR.205(c), GM1 IS.I/D.OR.205(c), AMC1 IS.I/D.OR.205(d), GM1 IS.I/D.OR.205(d), GM2 IS.I/D.OR.205(d), IS.I/D.OR.210.</i></p> <p><i>Pentru a facilita comparabilitatea reciprocă a evaluărilor de risc între organizații, atribuirea nivelului de risc conform punctului (e) de mai sus trebuie să țină cont de informațiile relevante obținute în coordonare cu organizațiile interconectate identificate conform punctului (b) de mai sus.</i></p> <p><i>Exemple tipice (neexhaustive) de interfețe conform punctului (b) de mai sus, pe care o organizație le poate avea cu alte organizații și care pot conduce la expunere reciprocă la riscuri privind securitatea informațiilor, pot fi următoarele:</i></p> <ul style="list-style-type: none"> – interfața AMO cu CAMO-uri care furnizează ordine de lucru, instrucțiuni pentru menținerea navigabilității (ICA), informații privind configurația aeronavelor, liste de elemente amânate, informații MEL etc.; – interfața cu OEM-uri și DOA-uri care oferă acces la instrucțiuni pentru menținerea navigabilității (ICA), instrucțiuni de reparație, software pentru actualizarea sistemelor avionice etc.; – interfața cu furnizori de piese, scule, echipamente de testare (inclusiv actualizări software pentru echipamentele de testare); – interfața cu contractori și subcontractori; 		

Autoritatea Aeronautică Civilă Română

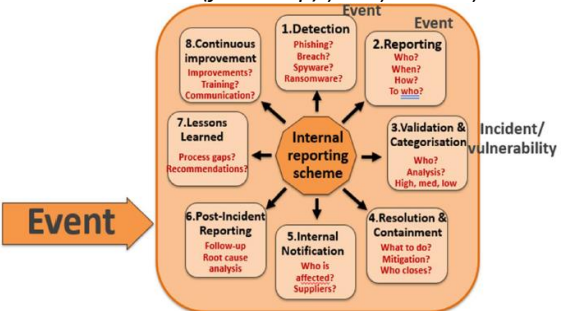
Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>(b) Procedura utilizată pentru identificarea interfețelor pe care organizația le are cu alte organizații și care ar putea duce la expunerea reciprocă la riscuri privind securitatea informațiilor.</p> <p>(c) Procedura utilizată pentru identificarea acelor riscuri de securitate a informațiilor, care pot avea un impact potențial asupra siguranței aviației. Notă: Dacă ISMM este un manual separat de Manualul SMS, se poate face referire la procesele și instrumentele descrise în SMSM.</p> <p>(d) Un tabel predefinit al nivelurilor de risc. Tabelul trebuie să ia în considerare probabilitatea apariției scenariului de amenințare (verosimilitatea) și severitatea consecințelor sale asupra siguranței. Pe baza aceluși tabel și ținând cont dacă organizația are un proces structurat și repetabil de management al riscurilor pentru operațiuni, organizația trebuie să poată stabili dacă riscul este acceptabil sau trebuie tratat în conformitate cu punctul IS.I/D.OR.210.</p> <p>(e) Procesul de atribuire a nivelului corespunzător de risc fiecărui risc de securitate a informațiilor identificat ca având un impact potențial asupra siguranței aviației, conform punctului (c) de mai sus, asociind fiecare risc și nivelul său cu elementul sau interfața corespunzătoare identificate în punctele (a) și (b) de mai sus.</p> <p>(f) Procedura utilizată pentru revizuirea și actualizarea evaluării riscurilor la intervale regulate sau atunci când apar oricare dintre următoarele situații:</p> <ol style="list-style-type: none"> (1) există o modificare a elementelor supuse riscurilor privind securitatea informațiilor; (2) există o modificare a interfețelor dintre organizație și alte organizații, sau a riscurilor comunicate de alte organizații; (3) există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analiza și clasificarea riscurilor; (4) au fost extrase lecții din analiza incidentelor de securitate a informațiilor. <p>Periodicitatea revizuirilor evaluării riscurilor trebuie documentată de către organizație și să includă:</p> <ul style="list-style-type: none"> – justificarea alegerii acestei periodicități; – data aprobării; și – informații privind responsabilul de risc (risk owner). <p>Notă: organizația trebuie să ia în considerare AMC1 IS.I/D.OR.205(c) 2.1.3 Responsabilități clare pentru persoanele însărcinate cu evaluarea riscurilor și decizia dacă un risc este acceptabil sau trebuie tratat.</p>	<p>– interfața cu echipele de întreținere ale producătorului;</p> <p>– interfața cu organizațiile de instruire a personalului de întreținere;</p> <p>– interfața cu organizațiile de instruire a personalului navigant;</p> <p>– interfața cu autoritatea competentă;</p> <p>–etc.</p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
☐	<p>2.2. Tratarea riscurilor de securitate a informațiilor</p> <p>(a) Procesul de tratare a riscurilor trebuie să atingă cel puțin unul dintre obiectivele enumerate la IS.I/D.OR.210(a).</p> <p>(b) Atunci când se stabilește conformitatea cu obiectivele prevăzute la punctele IS.I/D.OR.210(a)(1) și IS.I/D.OR.210(a)(2), organizația trebuie să țină cont de următoarele:</p> <p>(1) Măsurile dezvoltate în conformitate cu aceste puncte trebuie implementate în baza unui plan de tratare a riscurilor, care să includă priorități, obiective, termene și responsabili definiți pe baza riscului.</p> <p>(2) Trebuie identificate și asociate considerațiile privind ciclul de viață, pentru a asigura eficacitatea continuă a măsurilor de securitate a informațiilor, inclusiv în ceea ce privește schimbul de date cu alte entități.</p> <p>(3) Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor, în conformitate cu IS.I/D.OR.205(d), pentru a evalua dacă măsurile dezvoltate conform acestor puncte introduc noi riscuri inacceptabile.</p> <p>În acest capitol sunt incluse:</p> <p>(a) Procedura utilizată pentru a stabili măsuri destinate abordării riscurilor inacceptabile (identificate conform IS.I/D.OR.205), pentru a le implementa în timp util și pentru a verifica eficacitatea lor continuă.</p> <p>Aceste măsuri trebuie să permită organizației:</p> <ol style="list-style-type: none"> 1. să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare; 2. să reducă consecințele asupra siguranței aviației asociate materializării scenariului de amenințare; 3. să evite riscurile. <p>Aceste măsuri nu trebuie să introducă noi riscuri potențial inacceptabile pentru siguranța aviației.</p> <p>(b) Procedura utilizată pentru a informa persoanele menționate la punctele IS.I/D.OR.240(a) și (b), precum și alte categorii de personal afectat din cadrul organizației, cu privire la rezultatul evaluării riscurilor, scenariile de amenințare corespunzătoare și măsurile care trebuie implementate.</p> <p>Procedura trebuie să includă și obligația organizației de a informa acele organizații cu care are interfețe cu privire la orice risc comun identificat între ambele părți.</p> <p>Aspecte-cheie de luat în considerare la elaborarea procedurilor pentru „Tratarea riscurilor de securitate a informațiilor”:</p> <ul style="list-style-type: none"> • „Transferul de risc” nu este o măsură acceptabilă de tratare a riscurilor (de exemplu, abordarea riscului doar prin încheierea unei polițe de 	<p><i>IS.I/D.OR.200(a)(3); IS.I/D.OR.205; IS.I/D.OR.210; GM1 IS.I/D.OR.210; AMC1 IS.I/D.OR.210(a)</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>asigurare care acoperă pierderile financiare, fără a trata impactul asupra siguranței aviației).</p> <ul style="list-style-type: none"> • Exemple de măsuri acceptabile sunt, de exemplu: <ul style="list-style-type: none"> ○ Prevenirea riscului (de exemplu, introducerea unor măsuri de control al accesului, cum ar fi o politică de parole); ○ Atenuarea riscului (de exemplu, existența unui plan de răspuns la incidente, efectuarea de copii de siguranță ale datelor etc.); ○ Evitarea riscului (de exemplu, evitarea anumitor soluții tehnologice care creează riscuri și utilizarea unora mai robuste). • Măsurile de securitate a informațiilor adoptate nu trebuie să introducă riscuri noi potențiale pentru siguranța aviației. • Măsurile trebuie să fie bine comunicate, înțelese și aprobate de către managerul responsabil, care trebuie să asigure o comunicare eficientă în cadrul organizației. • Alte organizații care împart o interfață cu organizația trebuie informate cu privire la riscurile partajate și măsurile luate. • Măsurile trebuie implementate în timp util și verificate pentru eficacitatea lor continuă. 			
☐	<p>2.3 Schema internă de raportare a securității informațiilor</p> <p>Acest capitol trebuie să:</p> <p>l) descrie schema internă de raportare stabilită de organizație pentru colectarea și evaluarea evenimentelor de securitate a informațiilor, inclusiv a celor care trebuie raportate prin Schema de raportare externă (conform IS.I/D.OR.230).</p> <p>Această schemă internă de raportare, împreună cu procesul descris în Capitolul 2.4, trebuie să permită organizației să:</p> <ol style="list-style-type: none"> 1. identifice care dintre evenimentele raportate sunt considerate incidente sau vulnerabilități de securitate a informațiilor ce pot avea un impact potențial asupra siguranței aviației; 2. identifice cauzele și factorii contributivi ai incidentelor și vulnerabilităților de securitate a informațiilor identificate conform punctului (1) de mai sus și să le abordeze ca parte a procesului de management al riscurilor de securitate a informațiilor descris în capitolele 2.1 și 2.4; 3. asigure evaluarea tuturor informațiilor cunoscute și relevante referitoare la incidentele și vulnerabilitățile de securitate a informațiilor identificate conform punctului (1) de mai sus; 4. asigure implementarea unei metode de distribuire internă a informațiilor, după caz. 	<p>IS.I/D.OR.200(a)(4); IS.I/D.OR.215; AMC1 IS.I/D.OR.215(a)&(b); GM1 IS.I/D.OR.215(a)&(b); GM2 IS.I/D.OR.215(a)&(b); GM3 IS.I/D.OR.215(a)&(b); GM1 IS.I/D.OR.215(c); GM1 IS.I/D.OR.215(d)</p> <p>NOTĂ: Organizația poate decide să integreze conținutul aferent prezentului capitol 2.3 în capitolul din manualul organizației intitulat „Raportare și investigații interne privind siguranța”, asigurând corelarea cu cerințele de raportare din SMS. În cadrul acestei secțiuni vor fi incluse prevederi privind obligațiile de raportare către autoritățile competente, precum AIAS și DNSC, precum și specificarea platformelor și canalelor utilizate pentru transmiterea notificărilor, în concordanță cu procedurile interne de gestionare a incidentelor și cu cerințele legale aplicabile.</p> <p>Diagrama menționată (Figura 1) ilustrează un exemplu de proces intern de raportare, în care:</p>		

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>Această schemă internă de raportare trebuie să impună ca orice organizație contractată, care ar putea expune organizația la riscuri de securitate a informațiilor cu impact potențial asupra siguranței aviației, să raporteze evenimentele de securitate a informațiilor către organizație, transmitând aceste rapoarte prin procedurile stabilite în acordurile contractuale specifice.</p> <p>II) Să descrie modul în care organizația cooperează la investigații cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor pentru propriile activități.</p> <p>Procedurile descrise în acest capitol trebuie să specifice clar:</p> <ul style="list-style-type: none"> • cine sunt persoanele implicate; • care sunt rolurile și responsabilitățile acestora, în special în ceea ce privește: <ul style="list-style-type: none"> ○ evaluarea evenimentelor raportate; ○ decizia privind care dintre evenimente sunt considerate incidente și/sau vulnerabilități cu impact potențial asupra siguranței. <p>În cazul în care sistemul de raportare cerut conform IS.I/D.OR.215 este integrat unui sistem de raportare internă existent, organizația trebuie să se asigure de direcționarea corectă a rapoartelor și informațiilor conținute de acestea.</p>	<ul style="list-style-type: none"> • <i>evenimentele sunt detectate și raportate intern;</i> • <i>acestea sunt evaluate pentru a decide care dintre ele sunt considerate incidente/vulnerabilități cu impact potențial asupra siguranței;</i> • <i>apoi urmează diferite etape care acoperă: izolarea situației (containment), notificarea internă, analiza, urmărirea măsurilor (follow-up) și lecțiile învățate.</i> <div style="text-align: center;">  </div> <p style="text-align: center;"><i>Figura 1: Exemplu de proces intern de raportare</i></p>		
□	<p>2.4 Incidente de securitate a informațiilor – Detectare, răspuns și recuperare</p> <p>Acest capitol trebuie să descrie următoarele:</p> <p>(a) Procedura utilizată pentru implementarea măsurilor de detectare a incidentelor și vulnerabilităților care indică materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Aceste măsuri de detectare trebuie să permită organizației:</p> <ol style="list-style-type: none"> 1. să identifice abateri de la parametri funcționali de performanță prestabiliți; 2. să declanșeze alerte pentru activarea măsurilor corespunzătoare de răspuns, în cazul oricărei abateri. <p>(b) Procedura utilizată pentru implementarea măsurilor de răspuns la orice condiții ale unui eveniment identificate conform punctului (a), care pot evolua sau s-au dezvoltat deja într-un incident de securitate a informațiilor. Aceste măsuri de răspuns trebuie să permită organizației:</p> <ol style="list-style-type: none"> 1. să inițieze reacția la alertele menționate la punctul (a)(2), activând resursele și acțiunile predefinite; 	<p>IS.I/D.OR.200(a)(5); IS.I/D.OR.220; GM1 IS.I/D.OR.220; AMC1 IS.I/D.OR.220(a); GM1 IS.I/D.OR.220(a); AMC1 IS.I/D.OR.220(b); GM1 IS.I/D.OR.220(b); AMC1 IS.I/D.OR.220(c); GM1 IS.I/D.OR.220(b)&(c); GM1 IS.I/D.OR.220(c)</p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>2. să limiteze răspândirea unui atac și să evite materializarea completă a unui scenariu de amenințare;</p> <p>3. să controleze modul de cedare al elementelor afectate, conform definiției din punctul IS.I/D.OR.205(a).</p> <p>(c) Procedura utilizată pentru implementarea măsurilor de recuperare după incidentele de securitate a informațiilor, inclusiv măsurile de urgență, dacă este necesar.</p> <p>Aceste măsuri de recuperare trebuie să permită organizației:</p> <ol style="list-style-type: none"> 1. să elimine condiția care a cauzat incidentul sau să o restrângă la un nivel tolerabil; 2. să atingă o stare sigură a elementelor afectate, conform punctului IS.I/D.OR.205(a), într-un interval de timp de recuperare definit anterior de organizație. 			
☐	<p>2.5. Schema externă de raportare a securității informațiilor</p> <p>În cadrul aplicării schemei externe de raportare a securității informațiilor, organizația asigură conformitatea cu cerințele prevăzute de Regulamentul (UE) 376/2014 privind raportarea evenimentelor în aviație. Astfel, orice incident sau vulnerabilitate de securitate a informațiilor care poate reprezenta un risc semnificativ pentru siguranța aviației este raportat către AIAS și autoritatea competentă AACR și, după caz, către deținătorul autorizației de proiectare sau organizația responsabilă pentru proiectarea sistemului ori componentei afectate. Procedurile interne stabilesc clar responsabilitățile, metodele de raportare, termenele (notificarea inițială, raportarea în 72 de ore, raportul de urmărire), măsurile de confidențialitate și criteriile de evaluare a incidentelor, asigurând o structură unitară, completă și conformă atât cu SMS-ul organizației, cât și cu cerințele autorităților competente.</p> <p>Acest capitol trebuie să descrie schema de raportare externă a securității informațiilor implementată de organizație, pentru a se asigura că orice incident sau vulnerabilitate de securitate a informațiilor, care poate reprezenta un risc semnificativ pentru siguranța aviației, este raportat la autoritatea competentă</p> <ol style="list-style-type: none"> 1. Atunci când un astfel de incident sau o astfel de vulnerabilitate afectează o aeronavă sau un sistem ori componentă asociată, organizația trebuie, de asemenea, să îl raporteze către AIAS, AACR și, după caz deținătorului aprobării de proiectare (design approval holder). 2. Atunci când un astfel de incident sau o vulnerabilitate afectează un sistem sau o componentă utilizată de organizație, aceasta trebuie să îl raporteze organizației responsabile pentru proiectarea sistemului sau componentei respective. 	<p>IS.I/D.OR.200(a)(8); IS.I/D.OR.230; GM1 IS.I/D.OR.230; AMC1 IS.I/D.OR.230(a)&(b); GM1 IS.I/D.OR.230(a)&(b); AMC1 IS.I/D.OR.230(c); GM1 IS.I/D.OR.230(c)</p> <p><u>NOTE:</u></p> <p>1. Organizația poate decide să integreze conținutul aferent acestui capitol 2.5 în capitolul organizației intitulat „Raportarea evenimentelor (Occurrence Reporting)” din manualul de prezentare/ SMM/ etc.</p> <p>2. Reamintim organizației că prin OUG155/2024 sunt impuse cerințe de raportare către DNSC a incidentelor de securitate cibernetică</p> <p>3. Raportarea către AIAS (pentru evenimente reglementate de Regulamentul (UE) 376/2014) se realizează, în maxim 72 de ore, prin platforma națională ECCAIRS, accesibilă la: https://aias.gov.ro/</p> <p>Pentru a permite transmiterea raportului inițial în termen de 72 de ore, precum și a unui raport actualizat ulterior, dacă este necesar este necesară deținerea unui cont de utilizator</p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>Această schemă externă de raportare trebuie să includă:</p> <ol style="list-style-type: none"> 1. Transmiterea unei notificări către AIAS, AACR și, după caz, către deținătorul autorizației de proiectare sau către organizația responsabilă pentru proiectarea sistemului sau a componentei, imediat ce condiția a devenit cunoscută de către organizație; 2. Transmiterea unui raport către AIAS, AACR și, după caz, către deținătorul autorizației de proiectare sau către organizația responsabilă pentru proiectarea sistemului sau componentei, cât mai curând posibil, dar nu mai târziu de 72 ore de la momentul în care condiția a devenit cunoscută organizației, cu excepția cazurilor excepționale care împiedică acest lucru. <p>(3) Transmiterea unui raport de urmărire (follow-up) către AIAS, AACR și, după caz, către deținătorul certificatului de tip sau către organizația responsabilă pentru certificarea sistemului ori componentei, conținând detalii privind:</p> <ul style="list-style-type: none"> • acțiunile pe care organizația le-a întreprins sau intenționează să le întreprindă pentru recuperarea după incident; • acțiunile pe care intenționează să le implementeze pentru a preveni incidente similare de securitate a informațiilor în viitor. <p>Acest raport de urmărire trebuie transmis imediat ce aceste acțiuni au fost identificate.</p> <p>Cerințe procedurale:</p> <p>Procedurile descrise în acest capitol trebuie să specifice clar cine sunt persoanele implicate și care sunt rolurile și responsabilitățile acestora, în special în legătură cu:</p> <ul style="list-style-type: none"> • decizia privind incidentele și/sau vulnerabilitățile care trebuie raportate extern, deoarece pot reprezenta un risc semnificativ pentru siguranța aviației; • evaluarea acestor incidente și vulnerabilități; • pregătirea și aprobarea rapoartelor aplicabile, precum și transmiterea acestora către autoritatea competentă și, după caz, către deținătorul certificatului de tip și/sau către organizația responsabilă pentru certificarea sistemului ori componentei afectate. <p>Alte elemente obligatorii ale procedurii</p> <p>Procedurile trebuie, de asemenea, să specifice:</p> <ul style="list-style-type: none"> • metodele utilizate pentru raportare; • termenele de raportare, incluzând: <ul style="list-style-type: none"> ○ notificarea inițială, ○ raportul de urmărire / analiză, 			

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR						
	<ul style="list-style-type: none"> ○ închiderea investigației; • măsurile de confidențialitate introduse pentru a proteja identitatea persoanei care raportează și a celor menționate în rapoarte; • categoriile de stare ale rapoartelor, utilizate pentru a defini progresul și închiderea acestora. <p>Tabelul de mai jos (sau unul echivalent) trebuie inclus în prezentul capitol, iar una dintre stările de raportare enumerate mai jos trebuie selectată și completată atunci când este transmis un raport (inițial sau ulterior):</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">Închis la emitere</td> <td>Raport închis de către organizația care a raportat, încă de la prima emitere, dacă investigația este deja finalizată. (Justificarea pentru închidere trebuie inclusă în secțiunea narativă a raportului.)</td> </tr> <tr> <td>Deschis</td> <td>Raportul este încă deschis. A fost primită doar informarea inițială, iar investigația este în curs de desfășurare.</td> </tr> <tr> <td>Închis (după finalizarea evaluării)</td> <td>Evaluarea a fost finalizată, iar un plan de acțiune propus există și a fost implementat sau se află în curs de implementare.</td> </tr> </table> <ul style="list-style-type: none"> • Necesitatea ca rapoartele să conțină informații relevante și, acolo unde este posibil, evaluarea rezultatelor (dacă acestea sunt cunoscute); • Câmpurile obligatorii ale raportului trebuie completate integral; • Necesitatea de a lua în considerare evenimentele raportate de contractori, care pot fi relevante pentru evaluarea riscurilor de securitate a informațiilor; • Necesitatea transmiterii rapoartelor de urmărire (follow-up), care trebuie să includă detalii privind acțiunile pe care organizația intenționează să le întreprindă pentru a preveni apariția unor evenimente similare în viitor, imediat ce aceste acțiuni au fost identificate. 	Închis la emitere	Raport închis de către organizația care a raportat, încă de la prima emitere, dacă investigația este deja finalizată. (Justificarea pentru închidere trebuie inclusă în secțiunea narativă a raportului.)	Deschis	Raportul este încă deschis. A fost primită doar informarea inițială, iar investigația este în curs de desfășurare.	Închis (după finalizarea evaluării)	Evaluarea a fost finalizată, iar un plan de acțiune propus există și a fost implementat sau se află în curs de implementare.			
Închis la emitere	Raport închis de către organizația care a raportat, încă de la prima emitere, dacă investigația este deja finalizată. (Justificarea pentru închidere trebuie inclusă în secțiunea narativă a raportului.)									
Deschis	Raportul este încă deschis. A fost primită doar informarea inițială, iar investigația este în curs de desfășurare.									
Închis (după finalizarea evaluării)	Evaluarea a fost finalizată, iar un plan de acțiune propus există și a fost implementat sau se află în curs de implementare.									
<input type="checkbox"/>	<p>2.6 Contractarea activităților de securitate a informațiilor</p> <p>Acest capitol trebuie să includă următoarele:</p> <ul style="list-style-type: none"> • O listă a activităților de management al securității informațiilor care sunt contractate către alte organizații, împreună cu identificarea acestor organizații. • O descriere a modului în care organizația asigură că, în cazul contractării oricărei părți din activitățile de management al securității informațiilor menționate la punctul IS.I/D.OR.200 către alte organizații, activitățile 	<p><i>IS.I/D.OR.200(a)(9); IS.I/D.OR.235; GM1</i> <i>IS.I/D.OR.235; GM2 IS.I/D.OR.235; GM3</i> <i>IS.I/D.OR.235; AMC1 IS.I/D.OR.235(a); GM1</i> <i>IS.I/D.OR.235(a); GM2 IS.I/D.OR.235(a); AMC1</i> <i>IS.I/D.OR.235(b); GM1 IS.I/D.OR.235(b)</i></p>								

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>contractate respectă cerințele Part-IS, iar organizația contractată operează sub supravegherea organizației principale. Procedura trebuie să se asigure că riscurile asociate activităților contractate sunt gestionate corespunzător.</p> <ul style="list-style-type: none"> Capitolul trebuie să precizeze clar că organizația trebuie să adopte măsuri adecvate pentru a garanta că AACR are acces, la cerere, la organizația contractată, pentru a verifica conformarea continuă cu cerințele aplicabile stabilite prin Part-IS. Această cerință trebuie specificată explicit în contractele corespunzătoare. 			
☐	<p>2.7 Păstrarea înregistrărilor (Record-keeping) Acest capitol trebuie să descrie procedurile și măsurile implementate de organizație pentru a se asigura că:</p> <p>(a) Organizația păstrează înregistrările privind următoarele activități de management al securității informațiilor, pentru perioadele specificate:</p> <ol style="list-style-type: none"> Orice aprobare primită și evaluarea de risc asociată securității informațiilor, conform punctului IS.I/D.OR.200(e). → Aceste înregistrări trebuie păstrate cel puțin până la 5 ani după expirarea valabilității aprobării. Contractele pentru activitățile menționate la punctul IS.I/D.OR.200(a)(9). → Aceste contracte trebuie păstrate până la cel puțin 5 ani după modificarea sau încetarea contractului. Înregistrările proceselor esențiale menționate la punctul IS.I/D.OR.200(d). → Aceste înregistrări trebuie păstrate cel puțin 5 ani. Înregistrările riscurilor identificate în cadrul evaluării de risc menționate la IS.I/D.OR.205, împreună cu măsurile de tratare a riscurilor menționate la IS.I/D.OR.210. → Aceste înregistrări trebuie păstrate cel puțin 5 ani. Înregistrările incidentelor și vulnerabilităților de securitate a informațiilor, raportate conform schemelor de raportare prevăzute la punctele IS.I/D.OR.215 și IS.I/D.OR.230. → Aceste înregistrări trebuie păstrate cel puțin 5 ani. Înregistrările evenimentelor de securitate a informațiilor care pot necesita o reevaluare pentru a identifica eventuale incidente sau vulnerabilități nedetectate. → Aceste înregistrări trebuie păstrate până când evenimentele 	<p><i>IS.I/D.OR.200(a)(11); IS.I/D.OR.210; IS.I/D.OR.245; GM1 IS.I/D.OR.245; AMC1</i> <i>IS.I/D.OR.245(a)(1)(vi)&(a)(5); GM1</i> <i>IS.I/D.OR.245(a)(1)(vi)&(a)(5); AMC1</i> <i>IS.I/D.OR.245(c)&(d); GM1 IS.I/D.OR.245(c)&(d)</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>respective au fost reevaluate, conform unei periodicități definite într-o procedură stabilită de organizație.</p> <p>(b) Organizația păstrează înregistrările privind calificarea și experiența propriului personal implicat în activități de management al securității informațiilor, pentru perioadele specificate:</p> <ol style="list-style-type: none"> 1. Înregistrările de calificare și experiență ale personalului trebuie păstrate pe întreaga durată a activității acestuia în cadrul organizației și pentru cel puțin 3 ani după plecarea persoanei din organizație. 2. Personalul trebuie să aibă, la cerere, acces la propriile înregistrări individuale. În plus, la cererea acestora, organizația trebuie să le furnizeze o copie a propriilor înregistrări la încetarea contractului de muncă. <p>(c) Organizația trebuie să stocheze înregistrările menționate mai sus într-un mod care să asigure protecția împotriva deteriorării, modificării și furtului, iar informațiile trebuie identificate, atunci când este necesar, în funcție de nivelul de clasificare a securității. Organizația trebuie să se asigure că înregistrările sunt stocate prin mijloace care garantează:</p> <ul style="list-style-type: none"> • integritatea, • autenticitatea și • accesul autorizat la date. <p>Procedura inclusă în acest capitol trebuie să descrie formatul înregistrărilor menționate mai sus.</p>			
<input type="checkbox"/>	<p>2.8 Îmbunătățirea continuă (Continuous Improvement)</p> <p>Acest capitol trebuie să descrie modul în care organizația evaluează, utilizând indicatori de performanță adecvați, eficacitatea și maturitatea Sistemului de Management al Securității Informațiilor (ISMS).</p> <p>Această evaluare trebuie efectuată periodic, conform unei programări calendaristice predefinite de organizație sau după producerea unui incident de securitate a informațiilor.</p> <p>Dacă în urma evaluării efectuate se constată deficiențe, organizația trebuie să adopte măsuri de îmbunătățire necesare pentru a se asigura că ISMS continuă să respecte cerințele aplicabile și menține riscurile de securitate a informațiilor la un nivel acceptabil.</p> <p>De asemenea, organizația trebuie să reevalueze elementele ISMS afectate de măsurile adoptate.</p>	<p><i>IS.I/D.OR.200(b); IS.I/D.OR.260; AMC1 IS.I/D.OR.260; GM1 IS.I/D.OR.260; AMC1 IS.I/D.OR.260(a); GM1 IS.I/D.OR.260(a); AMC1 IS.I/D.OR.260(b); GM1 IS.I/D.OR.260(b)</i></p> <p>NOTĂ: <i>Pentru informații suplimentare privind evaluarea eficacității ISMS și evaluarea maturității ISMS, se accesează AMC1 IS.I/D.OR.260(a) și GM1 IS.I/D.OR.260(a).</i></p>		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
	<p>Aspecte-cheie de luat în considerare la elaborarea procedurilor pentru „îmbunătățire continuă”:</p> <ul style="list-style-type: none"> • Îmbunătățirea continuă este strâns legată de monitorizarea conformării. • Trebuie să existe un angajament ferm de a menține, și dacă este posibil, de a îmbunătăți nivelul de siguranță, având în vedere că atât mediul de securitate, cât și organizația evoluează constant. <p>Organizația trebuie să se adapteze dinamic la:</p> <ul style="list-style-type: none"> • vulnerabilități, actori de amenințare, instrumente și metode care apar constant și pot reduce eficacitatea controalelor existente; • modificări ale obiectivelor, arhitecturii, structurilor organizaționale și proceselor, care pot diminua nivelul de conformare. <p>Este esențial să se asigure că nu are loc o reducere a performanței. Pentru aceasta, trebuie utilizați Indicatori de Performanță (Key Performance Indicators – KPIs) care să măsoare dacă performanța scade și să evalueze eficacitatea și maturitatea ISMS.</p>			
☐	<p>2.9 Protecția confidențialității informațiilor primite de la alte entități</p> <p>Acest capitol trebuie să descrie procedurile utilizate de organizație pentru a proteja confidențialitatea oricărei informații pe care aceasta o poate primi de la alte organizații, în funcție de nivelul de sensibilitate al informației respective.</p> <p>În acest scop, organizația trebuie să stabilească un sistem de clasificare a informațiilor, corespunzător nivelului de sensibilitate al acestora, să implementeze și să mențină măsuri de securitate a informațiilor suficient de robuste și eficiente pentru a proteja informațiile și pentru a asigura aplicarea principiului „nevoii de a cunoaște” (adică limitarea accesului la informații doar pentru persoanele care au nevoie de ele în exercitarea atribuțiilor de serviciu).</p>	<p><i>IS.1/D.OR.200(a)(13); AMC1 IS.1/D.OR.200(a)(13)</i></p> <p><i>Organizația trebuie să protejeze sursa informațiilor în conformitate cu prevederile relevante stabilite în Regulamentul (UE) 2018/1139.</i></p> <p><i>De asemenea, aceasta trebuie să respecte Regulamentul (UE) nr. 376/2014.</i></p> <p>NOTĂ:</p> <p><i>Anumite informații/ înregistrări tratate în cuprinsul ISMM pot avea caracter sensibil.</i></p> <p><i>Drept urmare, organizația trebuie să dispună și de o procedură, parte integrantă a ISMS, prin care să se asigure că manipularea și difuzarea acestor informații este făcută:</i></p> <ul style="list-style-type: none"> - <i>cu respectarea cerințelor privind confidențialitatea și integritatea datelor</i> - <i>numai de către persoane care dețin calificarea și responsabilitatea pentru respectivele operațiuni, evaluate de către organizație în baza prevederilor IS.1/D.OR.240</i> - <i>în cuprinsul unor documente a căror circulație este controlată pentru respectarea restricțiilor de mai sus.</i> 		

Autoritatea Aeronautică Civilă Română

Conf.	Conținut	Referință reglementare/ notă explicativă	Observații/ Ref. ISMM ⁱ	AACR
		<i>Exemplu: Protecția informațiilor și a datelor manipulate prin analizele de risc, a rezultatelor acestora (registre de risc), a informațiilor transmise/primite de la organizațiile interfațate, etc.</i>		
☐	<p>2.10 Derogare</p> <p>Organizația trebuie să urmeze instrucțiunile furnizate în AMC1 IS.I/D.OR.205(a) și AMC1 IS.I/D.OR.205(b) pentru a efectua o evaluare documentată a riscurilor de securitate a informațiilor, în vederea obținerii aprobării din partea autorității competente pentru o derogare conform punctului IS.I/D.OR.200(e).</p> <p>Formularul F-CA-ISMM-DR-01 "Cerere de scutire de la aplicarea anumitor cerințe ale regulamentelor nr. UE 2023/203 și 2022/1645 (Part IS), în conformitate cu IS.I/D.OR.200(e)" poate fi accesat pe site-ul AACR</p> <p>Este necesară reevaluarea și actualizarea analizei de risc ori de câte ori intervin modificări față de condițiile inițiale pe baza cărora a fost acordată derogarea. Orice schimbare care poate afecta nivelul de securitate, structura proceselor, expunerea la vulnerabilități sau măsurile de control implementate trebuie analizată în mod riguros, pentru a asigura menținerea conformității cu cerințele normative aplicabile.</p> <p>În situația în care reevaluarea evidențiază modificări relevante sau potențiale impacturi asupra criteriilor avute în vedere la momentul autorizării derogării, operatorul/organizația are obligația de a informa în mod prompt autoritatea competentă și de a transmite documentația actualizată, astfel încât aceasta să poată reexamina valabilitatea derogării sau să poată dispune măsuri suplimentare, după caz.</p> <p>Autoritatea competentă este cea care stabilește dacă această evaluare este considerată satisfăcătoare pentru acordarea derogării.</p> <p>Organizația care dorește ca evaluarea riscurilor să fie realizată de o terță parte trebuie să ia în considerare cerințele prevăzute la IS.I/D.OR.235 și materialul de conformare asociat (AMC).</p>	<p>IS.I/D.OR.200(e), IS.I/D.OR.205(a), AMC1 IS.I/D.OR.205(b), AMC1 IS.I/D.OR.205(a), IS.I/D.OR.235</p> <p><u>NOTE:</u></p> <p>1) Pentru a justifica motivele care stau la baza unei derogări, evaluarea riscurilor trebuie să furnizeze explicații privind excluderea tuturor elementelor din domeniul de aplicare al ISMS.</p> <p>2) Această evaluare trebuie realizată prin raportare directă la Formularul F-CA-ISMM-DR-01 și la notele/condițiile menționate în documentația de aprobare inițială, pentru a asigura coerența între nivelul actual de expunere și criteriile luate în considerare la momentul acordării derogării.</p>		

Data evaluării conținutului ISMM	MANAGER CONFORMARE	
	Nume	Semnătură

CHECK-LIST ISMM

Secțiunea 4 Rezultatul evaluării AACR a conformării conținutului ISMM cu cerințele de reglementare aplicabile

Referința ISMM ¹ /		Ed./ rev. / data	
Denumirea organizației		Autorizare nr.	
Referința/ data transmiterii doc.			
Conformare conținut ISMM cu cerințele de reglementare	DA <input type="checkbox"/>	NU <input type="checkbox"/>	
Observații/ comentarii			
Denumire document (check-list) înregistrat în format electronic			
Inspector responsabil evaluare inițială	Nume		Semnătură/ Data finalizării
Inspector responsabil re-evaluare	Nume		Semnătură/ Data finalizării

¹ Referință ISMM sau a altor manuale ale organizației care descriu procedurile specifice ISMS