# Elementele care trebuie evaluate pentru nivelurile «Prezent» și «Adecvat» (inclusiv disponibilitatea de a începe operarea sistemului de management al securității informațiilor – ISMS)

(Aplicabil organizațiilor și autorității competente privind desfășurarea activităților de supraveghere a organizațiilor care implementează cerințele de Part-IS)

*Varianta în limba engleză a tabelului se regăsește în documentul*
*https://www.easa.europa.eu/community/system/files/2025-08/guidelines-part-is-oversight-approach-rev-august-2025.pdf*

| Cerințe reglementare | Elemente care trebuie evaluate pentru nivelurile „Prezent" și „Adecvat" (inclusiv gradul de pregătire pentru începerea operării ISMS) | Revizuire ISMM/ Manual organizație (MOE, CAME, etc) | Audit |
|---|---|---|---|
| **IS.I/D.OR.240 Structura organizațională** | a) A fost actualizată structura pentru a reflecta ISMS (de exemplu, desemnarea unui manager de securitate a informațiilor, structura de raportare)? | ● | |
| | ◦ Există o legătură între funcțiile de siguranță, securitate și securitatea informațiilor? | ● | ● |
| | b) În cazul în care organizația a decis să desemneze o Persoană Comună Responsabilă (CRP), are această persoană capacitatea și autoritatea delegată suficientă pentru implementarea eficientă a Part-IS în organizație? | ● | ● |
| | c)A elaborat organizația un cadru/politică pentru a aborda diferitele niveluri de încredere ale personalului? A fost deja evaluat personalul existent din perspectiva nivelului de încredere? | ● | ● |
| | d) A elaborat organizația un cadru de competențe și un proces de evaluare? A fost deja evaluat personalul existent pentru competență? | ● | ● |
| **IS.I/D.OR.200(a)(1) Politica de securitate a informațiilor** | a) A elaborat organizația o politică clar definită de securitate a informațiilor? | ● | |
| | ◦ Scopul politicii este clar enunțat? | ● | |
| | ◦ Sunt definite obiectivele de securitate a informației? | ● | |
| | ◦ Este conceptul de siguranță a aviației parte integrantă a politicii? | ● | |
| | ◦ Este conținutul politicii adecvat complexității organizației? | ● | ● |
| | ◦ Există o referire la schema organizației de clasificare a informațiilor? | ● | |
| | b) Politica este disponibilă pentru întregul personal / părțile contractate și a fost comunicată corespunzător? | | ● |
| | c) Au fost stabilite criterii pentru revizuirea politicii? | ● | ● |

| Cerințe reglementare | Elemente care trebuie evaluate pentru nivelurile „Prezent" și „Adecvat" (inclusiv gradul de pregătire pentru începerea operării ISMS) | Revizuire ISMM/ Manual organizație (MOE, CAME, etc) | Audit |
|---|---|---|---|
| **IS.I/D.OR.255 Managementul schimbărilor** | a) A fost elaborată o procedură de management al schimbărilor de către organizație și s-a solicitat aprobarea din partea autorității competente? | ● | |
| **IS.I/D.OR.235 Activități contractate de management al securității informațiilor** | a) Organizația a definit care sunt activitățile de management al securității informațiilor, dacă există, care sunt contractate către terți (Ref. IS.D/I.OR.235), și au fost stabilite contractele corespunzătoare? | ● | ● |
| | b) Există proceduri care definesc modul în care organizația supraveghează activitățile contractate de management al securității informațiilor și gestionează riscurile asociate? | ● | |
| | c) Organizația a asigurat accesul corespunzător al autorității competente la părțile contractate și a inclus această cerință în contractele aferente? | ● | ● |
| **IS.I/D.OR.205 (a) și (b) Domeniul de aplicare al ISMS** | a) A fost definit domeniul de aplicare al ISMS (de exemplu: servicii, sisteme, active, procese, interfețe, aria de acoperire/limite) cu justificări corespunzătoare pentru rezultate și eventualele excluderi? | ● | ● |
| **IS.I/D.OR.205 și 210 Managementul riscurilor** | a) A fost stabilit un proces formal de management al riscurilor privind securitatea informațiilor? | ● | |
| | ◦ Există definite cele trei procese principale (identificarea riscurilor, evaluarea riscurilor și tratarea riscurilor) în cadrul procesului de management al riscurilor? | ● | |
| | ◦Sunt definite clar criteriile de acceptare a riscurilor și responsabilitățile? | ● | |
| | b) A definit organizația modul în care vor fi gestionate riscurile asociate contractorilor / furnizorilor operaționali (fără a include activitățile de management al securității informațiilor contractate, acoperite de articolele IS.I.OR.235 și IS.D.OR.235, care sunt tratate mai jos în tabel)? | ● | ● |
| | c) A efectuat organizația o evaluare inițială a riscurilor (de exemplu, riscuri majore și scenarii de amenințare atât interne și la interfețe)? | ● | ● |
| | d) Dispune organizația de prevederi pentru un inventar al activelor (procese, software, hardware)? (de exemplu, șablonul descris în ISMM) | ● | |
| | e) A inclus deja organizația activele aplicabile în inventar? | | ● |
| | f) A fost stabilit un proces formal de management al riscurilor de securitate a informațiilor? | | ● |

| Cerințe reglementare | Elemente care trebuie evaluate pentru nivelurile „Prezent" și „Adecvat" (inclusiv gradul de pregătire pentru începerea operării ISMS) | Revizuire ISMM/ Manual organizație (MOE, CAME, etc) | Audit |
|---|---|---|---|
| **IS.I/D.OR.220 Managementul incidentelor (Detectare, Răspuns, Recuperare)** | a) Există proceduri implementate pentru detectarea incidentelor de securitate a informațiilor, inclusiv mecanisme de monitorizare pentru posibile amenințări? | ● | |
| | b) Există proceduri implementate pentru răspunsul prompt la incidentele detectate (de exemplu, măsuri inițiale de limitare a efectelor)? | ● | |
| | c) Există proceduri implementate pentru recuperarea după incidente și pentru restabilirea nivelului adecvat de siguranță după producerea unui incident? | ● | |
| | d) Măsurile implementate sunt adecvate și potrivite pentru a răspunde și a permite recuperarea informațiilor în urma incidentelor de securitate? | | ● |
| **IS.I/D.OR.215 și 230 Raportare internă și externă** | a) Există proceduri pentru raportarea evenimentelor din cadrul organizației și de la părțile externe? Personalul și părțile externe sunt informate cu privire la aceste proceduri? | ● | ● |
| | b) Există proceduri și responsabilități definite pentru evaluarea evenimentelor și pentru luarea deciziei privind clasificarea acestora ca incidente sau vulnerabilități? | ● | |
| | c) A elaborat organizația o procedură pentru a identifica ce incidente și vulnerabilități trebuie raportate prin sistemul de raportare externă? | ● | |
| | d) Au fost definite procedurile pentru raportarea externă (incluzând toate etapele procesului, raportare, analiză a cauzei rădăcină, urmărirea măsurilor etc.)? | ● | |
| | e) Personalul implicat în procesarea rapoartelor interne și externe este identificat, instruit și autorizat corespunzător? | | ● |
| **IS.I/D.OR.245 Păstrarea înregistrărilor** | a) Există proceduri care definesc ce înregistrări trebuie păstrate, perioada de păstrare și formatul acestora? | ● | |
| | b) A definit organizația măsuri adecvate pentru protecția înregistrărilor (de exemplu, împotriva deteriorării, modificării, furtului, accesului neautorizat etc.)? | ● | ● |
| **IS.I/D.OR.200(a)(6) și (a)(7) Măsuri și constatări notificate de autoritatea competentă** | a) A definit organizația proceduri pentru implementarea măsurilor notificate de autoritatea competentă ca reacție imediată la un incident de securitate a informațiilor sau la o vulnerabilitate cu impact asupra siguranței aviației? | ● | |
| | b) A definit organizația proceduri pentru tratarea constatărilor notificate de autoritatea competentă? | ● | |

| Cerințe reglementare | Elemente care trebuie evaluate pentru nivelurile „Prezent” și „Adecvat” (inclusiv gradul de pregătire pentru începerea operării ISMS) | Revizuire ISMM/ Manual organizație (MOE, CAME, etc) | Audit |
|---|---|---|---|
| **IS.I/D.OR.200(a)(13) Protecția confidențialității informațiilor primite de la alte organizații** | a) A definit organizația proceduri pentru protejarea confidențialității informațiilor primite de la alte organizații, în funcție de nivelul de sensibilitate al acestora? | ● | |
| **IS.I/D.OR.200(a)(12) Monitorizarea conformării cu cerințele Part-IS** | a) A pus organizația la dispoziție un raport intern de monitorizare a conformării, care descrie nivelul organizațional de conformare cu toate criteriile menționate în coloanele „ISMM” și „Audit” din prezentul checklist? | ● | |