NOTIFICARE DE NAVIGABILITATE

Număr: AACR-2025-0019

Data de emitere: 26.09.2025

Informare cu privire la implementarea prevederilor PART IS conform cerințelor

- regulamentului 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,[...]
- regulamentului 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, [...]

1. Scopul notificării

Prezentul document elaborat de AACR, detaliază punctul de vedere al AACR cu privire la cerințele Part-IS și oferă informații suplimentare față de AMC/GM-ul -Part-IS, în acord cu materialele de ghidare publicate de EASA*. Are rolul de a îndruma organizațiile autorizate de AACR în conformitate cu prevederile (EU) 1321/2014 Anexa II Part 145, Anexa Vc Part CAMO și prevederile (EU) 748/2012 Anexa I Part 21 subpartea G,

- în implementarea unui Sistem de Management al Securității Informațiilor (ISMS) în conformitate cu referințele legale menționate mai sus,
- în identificarea și evaluarea posibilelor derogări de la prevederile cadrului legislativ privind ISMS,
- în identificarea cerințelor obligatorii de raportare cu privire la incidentele și vulnerabilitățile de securitate a informațiilor cu impact în siguranța zborului.

**Notă: "Part IS Task Force" a fost creat sub coordonarea EASA, în scopul dezvoltării unei înțelegeri comune și a schimbului de experiențe privind aplicarea practică a regulamentelor, pentru identificarea soluțiilor comune (metode, procese, politici, opțiuni de implementare etc.) și convenirea asupra unei abordări armonizate privind implementarea prevederilor Part IS. Rezultatele acestei colaborări, publicate pe site-ul EASA, pot fi utilizate ca ghiduri atât de către organizațiile aeronautice, cât și de către autorități.*

AACR CONTACT
Şos. Bucureşti-Ploieşti, nr.38-40, RO-013695, Bucureşti, sector 1, România
Tel: +40.21.208.15.08, Fax:+40.21.208.15.72/ 21.233.40.62,
Telex: LRBBYAYA, BUHTOYA, www.caa.ro
e-mail: contact@caa.ro

Până în prezent, la adresa web: https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables , au fost publicate următoarele documente:

- *Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS*
- *Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)*
- *Part-IS Oversight Approach Guidelines*

De asemenea a fost dezvoltat un instrument pentru evaluarea conformării cu cerințele Part IS. Acesta poate fi accesat la următoarea adresă web:

https://www.easa.europa.eu/community/topics/part-compliance-assessment-tool

Subliniem faptul că prevederile Part-IS nu fac obiectul unei certificări independente, organizațiile ce intră în domeniul de aplicabilitate al Part-IS fiind evaluate ca parte a programului actual de supraveghere, conform autorizărilor deținute.

2. Excepții de la aplicabilitatea Part-IS

Prevederile PART IS nu sunt aplicabile organizațiilor care au domeniul de activitate limitat, așa cum este prezentat în tabelul de mai jos, situație în care nu sunt necesare activități ce au ca rezultat conformarea organizatiei cu prevederile acestui act normativ. Organizația are însă obligația de a evalua periodic cerințele PART IS luând în considerare faptul că acestea pot deveni aplicabile în cazul unor modificări produse în cadrul organizației.

Tip organizație	**domeniul autorizat**
Organizații Part 145	Exclusiv pentru întreținerea aeronavelor Part-ML
Organizații de managementul continuității navigabilității Part CAMO	Exclusiv pentru gestionarea aeronavelor Part-ML
Organizații de producție Part 21	Implicate exclusiv în producția de aeronave ELA 2

Notă: pentru detalii, consultați **Articolul 2 din Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei** și din **Regulamentul delegat (UE) 2022/1645 al Comisiei**.

3. Informații generale

Termenul „Part-IS” desemnează un set de reglementări europene având ca scop îmbunătățirea securității informațiilor (denumită, în general, securitate cibernetică) în sectorul aviației.

Aceste reglementări recunosc faptul că sectorul aviației este interconectat și vulnerabil la diverse amenințări privind securitatea informațiilor, inclusiv atacuri cibernetice, erori umane și deficiențe de proces. Prin implementarea Part-IS, Uniunea Europeană urmărește standardizarea și consolidarea practicilor de securitate a informațiilor, sporind astfel reziliența operațiunilor de aviație la amenințări și asigurând siguranța publică.

Se recomandă ca organizațiile să integreze aceste cerințe privind securitatea informațiilor în sistemele existente de management al siguranței aviației (SMS), asigurând o abordare coerentă și completă în gestionarea atât a riscurilor de siguranță, cât și a celor de securitate a informațiilor.

În peisajul digital dinamic de astăzi, securitatea informațiilor nu reprezintă doar o necesitate de business, ci un pilon al integrității organizaționale. Un ISMS (Sistem de Management al Securității Informațiilor) constituie un cadru structurat pentru gestionarea și protejarea datelor sensibile și critice pentru siguranță, asigurând conformitatea, reducerea riscurilor și încrederea părților interesate.

Un ISMS eficient oferă o abordare bazată pe risc în ceea ce privește securitatea informațiilor. Prin identificarea, analiza și reducerea riscurilor, organizația poate diminua vulnerabilitățile și poate răspunde rapid și eficient incidentelor. Implementarea unui ISMS promovează o cultură a securității informațiilor la toate nivelurile organizației. Instruirea, conștientizarea și responsabilitatea devin elemente esențiale, oferind angajaților capacitatea de a recunoaște și contracara eficient amenințările cibernetice.

Un ISMS nu este un cadru static, ci un proces continuu de îmbunătățire. Prin monitorizare periodică, audituri, evaluări și responsabilități clar definite, sistemul se adaptează la noi amenințări, tehnologii și cerințe de business, asigurând relevanța și reziliența.

Chiar dacă reglementările aplicabile se referă în principal la implicațiile pentru siguranța aviației, este logic ca un ISMS să includă întreaga structură organizațională și să acopere și alte aspecte, cum ar fi continuitatea afacerii, protecția datelor și procesele legate de securitatea aviației, acolo unde este cazul. Aceasta înseamnă că, din punct de vedere al conformității, doar implicațiile legate de siguranța aviației sunt relevante. Totuși, este în interesul organizației să includă în ISMS toate procesele care prezintă un risc potențial sau real pentru securitatea informațiilor.

4. Integrarea Part-IS în sistemul de management organizațional existent

Integrarea unui ISMS într-un sistem de management deja existent (de exemplu SMS) reduce redundanțele, luând în considerare faptul că ambele sisteme, în ciuda obiectivelor lor diferite, reprezintă abordări structurate și sistematice pentru gestionarea riscurilor. Dintr-o perspectivă organizațională, diferitele tipuri de riscuri interacționează între ele, iar implementarea anumitor măsuri de diminuare a riscurilor poate acoperi mai multe tipuri de riscuri.

AACR recomandă integrarea ISMS în cadrul unui sistem de management existent. 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

Obligația de a implementa Part-IS în cadrul unei organizații autorizate rezultă din cerințele specifice regulamentului în baza căruia s-a emis autorizarea organizației (de exemplu 145.A.200A / CAMO.A.200A / 21.A.139A / 21.A.239A / ... etc).

Termenul de conformare cu prevederile Part-IS diferă în funcție de actul normativ în baza căruia organizația a fost autorizată de către AACR. În prezent, AACR nu intenționează să efectueze audituri și/sau inspecții separate în avans pentru a verifica conformitatea organizației în ceea ce privește implementarea integrală a Part-IS. Responsabilitatea pentru implementarea la timp revine organizației, pe baza procesului de Management al Schimbării deja implementat, proces obligatoriu pentru fiecare organizație, prin sistemului de management a siguranței (SMS).

Modul de implementare și funcționare a ISMS este verificat de către AACR, ca parte a activității de supraveghere continuă, cu ocazia auditurilor planificate. În cazul identificării unor neconformități față de prevederile Part-IS în cadrul activității de supraveghere, acestea vor fi documentate corespunzător. Acest lucru ar trebui să permită organizației să atingă conformarea deplină prin soluționarea neconformităților (CAP, analiza cauzei rădăcină și a factorilor contributivi, acțiuni corective și preventive) utilizând procesele definite, deja stabilite.

După cum s-a menționat mai sus, AACR recomandă o abordare integrată pentru implementarea cerințelor Part-IS. Se recomandă o descriere integrată a sistemului de management care să includă Part-IS, structura manualelor existente fiind completată cu subiectele Part-IS. Alternativ, organizația poate să întocmească un Manual de Securitate a Informațiilor (ISMM) separat.

Tabelul 2 din documentul ”**EASA Guidelines Part-IS oversight approach”** enumeră unele dintre elementele ce trebuie implementate de către organizații pentru a fi pregătite să opereze ISMS.

4.1 Cerințe esențiale

În scopul unei bune înțelegeri, conceptele-cheie ale ISMS sunt detaliate în paragrafele următoare.

Politici și proceduri

Elaborarea unei politici, identificarea proceselor și elaborarea procedurilor specifice privind securitatea informațiilor reprezintă o cerință fundamentală, conform Part-IS.

Organizația trebuie să realizeze un inventar al tuturor sistemelor relevante, urmat de evaluarea riscurilor pentru potențialele amenințări și vulnerabilități identificate care pot avea impact asupra siguranței aviației. Evaluarea potențialelor amenințări și riscuri va avea în vedere diverse scenarii, inclusiv munca la distanță, utilizarea dispozitivelor mobile și gestionarea datelor sensibile, pentru a asigura o acoperire completă.

Documentul astfel creat stă la baza politicilor ce definesc poziția organizației cu privire la propriile active digitale și asigură faptul că personalul propriu poate înțelege modul adecvat de gestionare a acestor active.

Pe lângă politicile de utilizare acceptabilă, este esențial să fie elaborate planuri detaliate de răspuns la incidente. Aceste planuri trebuie să ofere instrucțiuni pas cu pas privind modul de detectare, raportare și gestionare a incidentelor de securitate a informațiilor. Ele trebuie să specifice rolurile și responsabilitățile în timpul unui incident, inclusiv comunicarea, investigarea, rezolvarea și persoanele decidente. Implementarea acestor planuri revine organizației. AACR nu impune utilizarea unor instrumente specifice. Dacă, de exemplu, o organizație decide că implementarea acestora în cadrul ERP-ului său este adecvată, acest lucru este acceptabil pentru autoritate.

Măsurile de control al accesului reprezintă un alt element esențial; aceste politici trebuie să definească modul în care accesul la sistemele informatice și la date este acordat, gestionat și revocat.

Trebuie stabilite linii directoare clare pentru protecția datelor, inclusiv criptarea, păstrarea și eliminarea sigură a datelor. Pentru a asigura eficiența acestor politici, acestea trebuie să fie ușor accesibile tuturor angajaților și revizuite periodic pentru a reflecta schimbările tehnologice, legislative și noile amenințări. Programe periodice de instruire și conștientizare trebuie desfășurate pentru a menține personalul informat conform celor mai recente practici de securitate.

Cartografierea interdependențelor

Cartografierea interdependențelor din cadrul organizației este un pas esențial în implementarea unui Sistem de Management al Securității Informațiilor (ISMS), conform cerințelor Part-IS.I/D.OR. Acest proces presupune identificarea și documentarea modului în care fiecare departament depinde de altele și de furnizorii externi de servicii. Înțelegerea acestor interdependențe este esențială pentru crearea unei strategii complete de management al riscurilor.

Se recomandă ca fiecare departament să își descrie funcțiile principale și resursele interne și externe de care depinde pentru desfășurarea activităților. Aceasta include identificarea sistemelor software, a informațiilor, a fluxurilor de date și a serviciilor terților care susțin activitățile zilnice.

Partea-IS.I/D.OR.235 pune un accent special pe rolul furnizorilor externi de servicii, cum ar fi furnizorii de software și companiile de outsourcing, în cadrul securității informațiilor organizației. La cartografierea acestor interdependențe, este important să se evalueze postura de securitate a acestor parteneri externi și să se verifice dacă aceștia fac obiectul cerințelor Part-IS.

Trebuie evaluate politicile, practicile și controalele lor de securitate a informațiilor pentru a se asigura că acestea corespund standardelor organizației și cerințelor de reglementare. Conform GM1 IS.I/D.OR.205(b), interfețele cu terți precum furnizorii de servicii și lanțurile de aprovizionare, trebuie identificate pe baza schimbului de date și informații, deoarece acestea pot duce la riscuri sporite de securitate a informațiilor prin expuneri reciproce.

Contractele cu acești furnizori trebuie să includă clauze care să impună respectarea cerințelor de securitate și să permită audituri pentru a verifica respectarea acestor standarde.

Managementul riscurilor

În faza inițială de implementare a Part-IS, efectuarea unor evaluări detaliate ale riscurilor este esențială pentru identificarea riscurilor de securitate a informațiilor care ar putea afecta siguranța aviației.

Primul pas este constituirea unei echipe dedicate, cu reprezentanți din diverse departamente, inclusiv IT, instruire, mentenanță, financiar, resurse umane și management, etc.

Această echipă trebuie să efectueze o analiză cuprinzătoare a tuturor sistemelor de tehnologia informației și comunicațiilor și a datelor, pentru a identifica vulnerabilitățile și amenințările potențiale. Rezultatele se documentează într-un registru al riscurilor, clasificând riscurile în funcție de impactul potențial și de probabilitatea de apariție. Această abordare structurată asigură identificarea și prioritizarea eficientă a tuturor riscurilor posibile.

După finalizarea evaluării inițiale a riscurilor, pasul următor este elaborarea și implementarea planurilor de tratare a riscurilor pentru a reduce riscurile identificate. Acest lucru implică selectarea controalelor și măsurilor adecvate pentru fiecare risc, în funcție de severitatea acestuia.

- Pentru riscurile tehnice: se pot implementa soluții precum firewall-uri, criptare, managementul parolelor și sisteme de detecție a intruziunilor.
- Pentru riscurile legate de procese: se pot introduce îmbunătățiri precum audituri periodice, protocoale de răspuns la incidente și măsuri de control al accesului.

Toate măsurile de reducere a riscurilor trebuie gestionate în cadrul ISMS. Planurile trebuie revizuite și actualizate regulat, pentru a se adapta la noile amenințări și la schimbările din mediul organizațional, menținând o abordare proactivă în managementul securității informațiilor.

Detectarea, răspunsul și recuperarea în cazul incidentelor de securitate a informațiilor

Stabilirea unor mecanisme robuste de detectare, răspuns și recuperare a incidentelor de securitate a informațiilor este esențială pentru protejarea activelor informaționale ale organizației.

- **Detectare:** Se recomandă instalarea și configurarea unor instrumente avansate de monitorizare, capabile să identifice amenințări potențiale (tentative de acces neautorizat, activități malware, etc.). O echipă desemnată (internă sau externalizată) trebuie să monitorizeze constant aceste alerte pentru a asigura o detectare rapidă.
- **Răspuns:** Trebuie elaborat un plan clar de răspuns la incidente, care să detalieze pașii de urmat după identificarea unei amenințări, inclusiv acțiuni imediate pentru limitarea acesteia și prevenirea extinderii daunelor.
- **Recuperare:** Procedurile trebuie să includă rolurile și responsabilitățile personalului implicat, evaluarea impactului, delimitarea ariei afectate, identificarea sistemelor și datelor compromise, măsuri de izolare, eliminarea elementelor malițioase și

restaurarea sistemelor și datelor la starea normală de funcționare. Toate acțiunile trebuie documentate pentru analiză și raportare ulterioară.

Trebuie dezvoltat un plan de continuitate a afacerii, care să includă strategii pentru menținerea operațiunilor esențiale și a siguranței zborului pe durata incidentului, reducerea perturbărilor și revenirea rapidă la normalitate. Aceste proceduri trebuie testate și actualizate periodic prin simulări și exerciții practice, pentru a asigura eficiența lor în scenarii reale.

Instruire și conștientizare

Unul din elementele esențiale în securitatea informațiilor este **factorul uman**. Chiar dacă în multe situații este necesară o cunoaștere tehnică aprofundată în domeniul IT, este recunoscut pe scară largă că unul dintre cele mai vulnerabile puncte din securitatea unei organizații îl reprezintă personalul. **Eroarea umană, lipsa de conștientizare și instruirea insuficientă** pot conduce la probleme majore de securitate.

Cerințele privind personalul reprezintă o componentă esențială a Sistemului de Management al Securității Informațiilor (ISMS), conform IS.I/D.OR.240.

În faza inițială de implementare, este esențial să fie dezvoltat un program cuprinzător de instruire care să acopere toate aspectele de securitate a informațiilor relevante pentru organizație. Acest program trebuie conceput pentru a oferi tuturor angajaților – inclusiv celor care nu sunt direct implicați în implementarea Part-IS – cunoștințele și competențele necesare pentru a respecta procedurile ISMS.

Se recomandă efectuarea unei analize a necesităților de instruire, pentru a identifica lipsa cunoștințelor și cerințele de pregătire pentru diferite funcții din cadrul organizației. Pe baza acestei analize, se dezvoltă module de instruire adaptate, care să abordeze subiecte precum: recunoașterea tentativelor de ”phishing”, practici corecte de gestionare a datelor cu caracter personal și importanța respectării protocoalelor de securitate.

Pentru menținerea unui nivel ridicat de conștientizare în rândul personalului, pot fi utilizate sesiuni periodice de instruire, ateliere de lucru și module e-learning. De asemenea, trebuie implementate evaluări periodice și cursuri recurente, pentru a asigura faptul că angajații rămân la curent cu cele mai recente practici și amenințări în domeniul securității.

Raportare și îmbunătățire continuă

Menținerea unor evidențe complete privind incidentele de securitate a informațiilor și acțiunile întreprinse este esențială pentru eficiența Sistemului de Management al Securității Informațiilor (ISMS).

În faza inițială de implementare, trebuie stabilite mecanisme interne solide de raportare, care să asigure comunicarea promptă a incidentelor în cadrul organizației. O legătură formală între funcțiile de securitate a informațiilor și cele de siguranță este esențială.

Aceasta presupune elaborarea unui protocol clar și accesibil, pe care toți angajații să-l poată urma pentru a raporta potențiale probleme de securitate. Fiecare incident trebuie documentat cu atenție, incluzând natura incidentului, acțiunile întreprinse ca răspuns și rezultatele obținute. Această documentare nu doar că ajută la o mai bună înțelegere a incidentului, dar oferă și date valoroase pentru analiza tendințelor și identificarea

problemelor recurente. Evidențele trebuie păstrate în siguranță și trebuie să poată fi accesate ușor pentru referințe viitoare, audituri de conformitate și analize.

Pe lângă raportarea internă, este obligatoriu să fie raportate incidentele semnificative către autoritățile competente, conform cerințelor IS.I/D.OR.230. Aceasta asigură transparența și conformitatea cu cerințele legale, contribuind la consolidarea încrederii cu organismele de reglementare și părțile interesate. Detalii privind cerințele legale și procesul de raportare asociat, sunt descrise la capitolul „Procesul de raportare”.

Politicile, procedurile și controalele trebuie revizuite și actualizate periodic, pe baza lecțiilor învățate din incidentele anterioare și a evoluției amenințărilor. Se recomandă efectuarea de audituri și evaluări periodice pentru a verifica eficiența măsurilor de securitate și a identifica domeniile care necesită îmbunătățiri. Totodată, trebuie încurajată o cultură a feedbackului în cadrul organizației, astfel încât angajații să poată sugera îmbunătățiri și să raporteze vulnerabilități potențiale fără teamă de represalii.

4.2 Aprobarea ISMM

Dacă organizația alege să elaboreze un ISMM separat, ediția inițială trebuie aprobată de AACR, conform cerințelor Part-IS, punctul IS.I/D.OR.250(b). Totuși, așa cum este descris la punctul 5, metoda preferată este integrarea conținutului ISMM în alte manuale (de exemplu, SMM/ MOE/ CAME etc) deja existente în cadrul organizației.

Dacă anumite subiecte specifice Part-IS sunt descrise în alte manuale de prezentare (de exemplu CAME, MOE, POE etc.), aceste modificări trebuie gestionate prin intermediul procedurii de tratare a modificărilor, definită în manualul de prezentare (→ Modificările necesită aprobare prealabilă).

Pentru a sprijini organizațiile în obținerea conformității inițiale, AACR va publica pe pagina web la adresa https://www.caa.ro/ro/pages/formulare-dn%20, punctul 15. ”Conformare cu cerintele PART IS”, o listă de verificare a conformității.

4.3 Transmiterea documentației

Din cauza volumului ridicat de solicitări așteptat, AACR solicită organizațiilor vizate să transmită prin intermediul platformei portal.caa.ro și conform proceselor AACR aplicabile, documentația Part IS, cu cel puțin **90 de zile înainte de data aplicabilității**, pentru a permite procesarea acesteia în timp util.

Documentele care trebuie transmise:

- Managementul schimbărilor (inclusiv planul de implementare, cu termene și responsabili)
- ISMM sau manualul de prezentare actualizat (CAMO/AMO/POE, etc), în cazul în care ISMM este integrat în documentația existentă;
- Autoevaluarea efectuată în cadrul organizației (Lista de verificare a conformității Part-IS).

5. Derogare

AACR recunoaște posibilitatea ca o organizație să obțină o aprobare pentru a **nu implementa cerințele Partea-IS**, în conformitate cu IS.I/D.OR.200(e) și va sprijini o astfel de cerere ori de câte ori este posibil și adecvat.

În acest demers, AACR se bazează nu doar pe reglementare, ci și pe ghidul suplimentar emis de EASA pentru aplicarea derogărilor, acolo unde acesta este adecvat și aplicabil

Fără a aduce atingere obligației de respectare a cerințelor de raportare prevăzute în Regulamentul (UE) nr. 376/2014(1) și a cerințelor din punctul IS.I/D.OR.200(a)(13), organizația poate primi aprobarea AACR de a **nu aplica cerințele prevăzute la punctele (a) – (d)** și cerințele conexe prevăzute la punctele IS.I/D.OR.205 – IS.I/D.OR.260, dacă demonstrează, spre satisfacția AACR, că activitățile, facilitățile, resursele și serviciile pe care le desfășoară, le furnizează, le primește și le menține **nu prezintă un risc de securitate a informațiilor cu impact potențial asupra siguranței aviației**, nici pentru ea însăși, nici pentru alte organizații. Aceasta este considerată o derogare.

Aprobarea AACR se bazează pe **o evaluare documentată a riscului de securitate a informațiilor**, care trebuie realizată de organizație sau de o terță parte, conform punctului IS.I/D.OR.205, verificată și aprobată de AACR, după caz. Evaluarea riscurilor poate fi realizată și documentată utilizând procedura existentă de evaluare a riscurilor din cadrul organizației sau prin intermediul șabloanelor puse la dispoziție de AACR pentru evaluarea derogării. Riscurile rezultate, dacă există, trebuie identificate și monitorizate în registrul de riscuri al organizației.

Valabilitatea continuă a acestei aprobări de derogare va fi revizuită de AACR în cadrul ciclului de supraveghere și ori de câte ori există o modificare a domeniului de activitate al organizației.

Evaluarea riscului conform IS.I/D.OR.205 al unei organizații constituie fundamentul pe baza căruia AACR decide dacă respinge sau acceptă o cerere de derogare. Pe lângă evaluarea riscului, sunt luate în considerare și alte aspecte, precum:

Considerații la nivel înalt privind expunerea în domeniul aviației:

- poziția organizației în cadrul lanțului funcțional al aviației;
- nivelul său de contribuție la consecințele asupra siguranței.

Considerații detaliate privind informațiile legate de siguranță, procesate sau produse:

- serviciile pe care organizația le furnizează și le primește, inclusiv interfețele acestora;
- procesele pe care organizația le-a stabilit pentru a furniza și primi aceste servicii.

Pentru a sprijini organizațiile în evaluarea cererilor lor, AACR va dezvolta **criterii și condiții de bază** care oferă o indicație asupra șanselor ca o solicitare pentru derogare întocmită corespunzător, să aibă succes.

Chiar dacă, în principiu, orice organizație aflată în domeniul de aplicare al Part-IS poate solicita o derogare, AACR va **tria cererile** pe baza criteriilor și condițiilor menționate,

înainte de a trece la o evaluare detaliată. Fiecare cerere a unei organizații va fi evaluată individual.

Notă: **cererile de derogare parțială** de la cerințe(articole) individuale nu sunt posibile.

5.1 Cererea de derogare

O cerere de derogare trebuie transmisă la AACR prin intermediul platformei portal.caa.ro, în conformitate cu procesele aprobate aferente autorizațiilor corespunzătoare.

Se recomandă ca organizațiile care dețin mai multe aprobări să ia legătura cu **toate departamentele relevante ale AACR** înainte de a transmite cererea.

Etape de urmat:

1. Transmiterea unei cereri de derogare, în conformitate cu procedura aprobată.
    - organizația trebuie să furnizeze informații referitoare la următoarele aspecte:
        - Aprobările afectate pentru care se solicită derogarea;
        - Justificarea excluderii prevederilor;
        - Prezentarea generală a serviciilor pe care organizația le furnizează și le primește;
        - Prezentarea generală a arhitecturii sistemelor informatice utilizate pentru desfășurarea activităților;
        - Informații despre modul în care se intenționează efectuarea evaluării inițiale a riscului de securitate a informațiilor, în corelare cu arhitectura de mai sus.
        - Informații privind metodologia care va fi utilizată pentru efectuarea evaluării riscului de securitate a informațiilor;
        - Lista persoanelor și a rolurilor care urmează să fie implicate în procesul de evaluare a riscului de securitate a informațiilor;
        - Identificarea terților care urmează să fie implicați în evaluarea riscului de securitate a informațiilor.

    Notă: AACR va publica pe pagina web: caa.ro un formular pentru cererea de derogare de la aplicarea unor cerințe Part-IS, în conformitate cu IS.I/D.OR-200 (e)
2. În plus, organizația trebuie să transmită informații mai detaliate, precum un **inventar al activelor TIC** (tehnologia informațiilor și comunicării) și o **evaluare a riscurilor**. Pentru a accelera procesul, AACR recomandă utilizarea șabloanelor dedicate puse la dispoziție (https://www.caa.ro/ro/pages/formulare-dn%20, punctul 15. ”Conformare cu cerințele PART IS”)
3. AACR va tria solicitările în funcție de condițiile prezentate în tabelul de mai jos. Organizația va primi **decizia AACR** prin inspectorul desemnat, la finalizarea procesului de evaluare.

Notă: Analiza de tip ”*case-by-case”* pentru o solicitare se referă întotdeauna la activitățile reale ale organizației. Prin urmare, o **analiză internă detaliată (analiza de risc)** trebuie furnizată împreună cu cererea.

Exemple de situații pentru evaluarea derogării

Condiții	Aprobări afectate
1.Servicii și produse critice sau legate de siguranță ale organizației nu sunt furnizate prin procese și informații digitale	
1.A Durata de viață sau timpii de utilizare a materialelor, componentelor și/sau intervalele de mentenanță nu sunt monitorizate integral digital printr-un sistem găzduit extern.	POA, MOA
2. Dependenta de terți în ISMS	
2.A Nu există înregistrări digitale de mentenanță sau organizația nu depinde de software sau platforme terțe (ex. AMOS, CAMP, Blue Eye), care sunt deja certificate sau gestionate prin procese conforme ISMS.	MOA, CAMO[1]
3. Suprafață de atac redusă *(**minimizarea numărului de puncte de intrare sau vulnerabilități** pe care un atacator le poate exploata într-un sistem).*	
3.A O mare parte din sistemele de mentenanță, CAMO și producție sunt offline și au expunere minimă sau inexistentă la rețeaua publică.	POA, MOA, CAMO[1]
3.B Sistemele OT (Operating Technology) nu sunt sau sunt doar minimal interconectate cu sistemele IT și nu sunt conectate la rețeaua publică.	POA/ MOA
3.C Nu există unelte de calibrare sau standuri de test interconectate. *MOA / POA*	MOA/ POA
3.D Sistemele de producție CNC pentru piese critice și structurale ale aeronavei nu sunt conectate la internet.	POA/ MOA
3.E Organizația nu operează aplicații web care au o influență directă sau indirectă asupra sistemelor sale productive.	POA, MOA, CAMO[1]

*Nota 1. **„stand-alone”** sau alt tip de CAMO (de exemplu, în cadrul Part-SPO sau Part-NCC) care **nu este integrat într-un AOC** (în conformitate cu Part-CAT)*

Nota 2. O cerere de derogare este cel mai probabil respinsă de AACR dacă un CAMO este incorporat într-un AOC. Nu există niciun AOC fără un CAMO. Din acest motiv, un CAMO aflat într-un sistem de management cuprinzător (inclusiv ISMS) nu poate solicita derogare individuală de la cerințele Partea-IS, chiar dacă criteriile menționate mai sus se aplică CAMO-ului. Riscul de securitate a informațiilor nu provine doar din activitățile CAMO, ci trebuie privit din perspectiva întregului AOC. O derogare ar fi posibilă doar dacă AOC-ul ar fi obținut aprobarea AACR pentru derogare (adică numai operațiuni VFR / operațiuni exclusiv cu aeronave ne-complexe).

6. Raportarea incidentelor și vulnerabilităților de securitate a informațiilor

Așa cum s-a menționat la cerințe esențiale la punctul **5.1**, menținerea unor evidențe complete privind incidentele de securitate a informațiilor și acțiunile întreprinse este esențială pentru eficiența Sistemului de Management al Securității Informațiilor.

6.1 Raportare internă

Trebuie stabilite procese și proceduri interne clare pentru ca personalul să raporteze evenimente de securitate a informațiilor observate sau suspectate. Procedurile și

responsabilitățile trebuie să fie definite pentru evaluarea evenimentelor și decizia asupra celor care trebuie considerate incidente sau vulnerabilități. Aceasta încurajează o cultură proactivă a securității în cadrul organizației.

Următoarele exemple (neexhaustive) descriu unele incidente de securitate a informațiilor care pot reprezenta motive pentru raportarea internă:

- **Acces neautorizat:** orice situație în care o persoană sau un sistem neautorizat obține acces la date sau alte sisteme;
- **Breșă de date:** expunerea informațiilor confidențiale către părți neautorizate, accidental sau prin acțiuni rău intenționate;
- **Infecție cu malware:** detectarea de viruși, viermi, ”ransomware” sau alte programe malițioase în rețeaua sau dispozitivele organizației;
- **Atac de tip ”phishing”:** încercări de a înșela angajații pentru a furniza informații sensibile prin e-mailuri sau site-uri frauduloase;
- **Pierderea sau furtul de dispozitive:** incidente ce implică pierderea sau furtul de laptopuri, telefoane mobile sau alte dispozitive care conțin informații sensibile;
- **Modificări neautorizate:** schimbări neaprobate în software, date sau configurații de rețea;
- **Compromiterea conturilor de utilizator:** detectarea unor conturi care au fost accesate sau folosite fără autorizare;
- **Activitate suspectă în rețea:** tipare neobișnuite de trafic de rețea care pot indica o amenințare de securitate;
- **Inginerie socială:** tentative de a manipula angajații pentru a divulga informații confidențiale sau a întreprinde acțiuni care compromit securitatea;
- **Încălcări ale politicilor:** cazuri în care angajații sau contractanții încalcă politicile sau procedurile de securitate ale organizației;
- **Vulnerabilități de securitate a informațiilor:** identificarea de slăbiciuni în software, hardware sau configurațiile de rețea care ar putea fi exploatate de atacatori;
- **Amenințări interne:** acțiuni rău intenționate sau neglijente ale angajaților sau contractanților care compromit securitatea informațiilor organizației;
- **Eșecul controalelor de securitate:** detectarea unor controale de securitate care nu au funcționat conform așteptărilor, expunând potențial organizația la risc.

6.2 Raportare externă

Organizațiile trebuie să notifice AIAS și AACR despre incidentele semnificative, în special cele cu potențial impact asupra siguranței, în termenele specificate. Trebuie elaborate proceduri pentru a identifica ce incidente și vulnerabilități trebuie raportate extern.

Următoarele exemple (neexhaustive) descriu unele incidente de securitate a informațiilor care pot constitui motive pentru raportarea internă (IS.I/D.OR.215) și externă către AIAS/ AACR și, dacă este cazul, către deținătorul aprobării de proiectare (IS. I/D.OR.230):

- Toate exemplele menționate anterior, considerate ca având un potențial impact asupra siguranței aviației;

- **Deturnare de la distanță:** obținerea accesului și controlului asupra unui sistem critic al aviației, ceea ce duce la compromiterea informațiilor;
- **Atacuri asupra lanțului de aprovizionare:** compromiterea lanțului de aprovizionare cu piese de aeronave poate duce la introducerea de componente defecte sau ”malware”, afectând siguranța aeronavei;
- **Compromiterea sistemului de mentenanță:** acces neautorizat la înregistrările de mentenanță ale aeronavelor poate duce la date incorecte sau falsificate, ceea ce poate genera defecțiuni mecanice;
- **Breșă în sistemul de divertisment la bord (IFE):** deși destinat utilizării de către pasageri, un atac asupra IFE poate oferi o cale de acces către sisteme mai critice ale aeronavei, reprezentând un risc de securitate;
- **”Hacking” asupra ACARS (Aircraft Communication Addressing and Reporting System):** accesul neautorizat la ACARS poate permite manipularea planurilor de zbor și a comunicațiilor dintre aeronave și stațiile de la sol, ceea ce poate provoca erori de navigație și riscuri pentru siguranță;
- **Manipularea FMS (Flight Management System):** atacurile cibernetice asupra FMS pot altera rutele de zbor, calculele de combustibil și alți parametri critici ai zborului, punând în pericol siguranța operațiunilor aeronavei.

6.3 Raportarea vulnerabilităților

AACR nu se așteaptă și nici nu recomandă raportarea pe scară largă a vulnerabilităților cunoscute din cadrul componentelor software (sisteme de operare și aplicații). Totuși, dacă o organizație detectează vulnerabilități cu **potențial impact asupra siguranței** și/sau cu un caracter de **noutate**, raportarea conform IS.OR.230 este obligatorie.

Următoarele exemple (neexhaustive) descriu unele vulnerabilități care pot constitui motive pentru raportarea internă (IS.OR.215) și externă către AIAS/AACR și, dacă este cazul, către deținătorul aprobării de proiectare (IS.OR.230):

- Vulnerabilități cunoscute pe scară largă într-un sistem informatic critic (sistem de operare, aplicație), afectând integritatea și/sau disponibilitatea și care nu pot fi atenuate;
- **Controale de acces slabe:** controale de acces inadecvate care pot permite persoanelor neautorizate să obțină acces la sisteme și date critice;
- **Exploatări potențiale ale comunicațiilor wireless:** vulnerabilități în sistemele de comunicații wireless utilizate pentru operațiunile aeronavelor, care pot fi exploatate pentru a perturba sau manipula transmisia datelor;
- **Sisteme învechite și nesuportate:** expuse la rețeaua publică, pot să nu dispună de caracteristicile moderne de securitate, devenind mai vulnerabile la atacuri cibernetice;
- **Componente sau software compromise provenite de la furnizori:** detectarea unor elemente care introduc vulnerabilități în sistemele aviatice.

6.4 Colaborarea între părțile interesate

Informațiile relevante despre incidente trebuie împărtășite cu alte entități din ecosistemul aviatic, pentru a spori reziliența colectivă în materie de securitate.

Tot personalul implicat trebuie să fie instruit corespunzător cu privire la procedurile respective și la procesarea/gestionarea rapoartelor.

7. Certificarea ISO/IEC 27001

O organizație care deține o certificare ISO/IEC 27001 valabilă **nu este automat conformă** cu cerințele Part-IS, chiar dacă cerințele pentru un ISMS specificate de Part-IS sunt, în cea mai mare parte, consistente și aliniate cu ISO/IEC 27001.

Totuși, Part-IS introduce prevederi specifice **contextului siguranței aviatice**. Dacă un ISMS bazat pe ISO/IEC 27001 este deja operat de o entitate pentru un alt domeniu sau context, acesta poate fi adaptat și extins la domeniul și contextul Part-IS pe baza unei analize a domeniului și a lacunelor existente.

Pentru ca o certificare ISO/IEC 27001 să fie valorificată în vederea obținerii conformității cu Part-IS, **siguranța aviației trebuie inclusă în managementul riscurilor organizației**, cu nivelul de acceptare a riscului determinat conform cerințelor aplicabile.

De asemenea, pentru o corespondență între principalele sarcini cerute de Part-IS și clauzele și controalele asociate din ISO/IEC 27001, se face trimitere la Anexa II din AMC & GM publicat pentru Partea-IS (Acceptable Means of Compliance and Guidance Material).