Consiliul
Uniunii Europene

Bruxelles, 18 iulie 2022
(OR. en)

11468/22
ADD 1

AVIATION 171
DELACT 120

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	14 iulie 2022
Destinatar:	Secretariatul General al Consiliului
Nr. doc. Csie:	C(2022) 4882 final - ANNEX
Subiect:	ANEXĂ la REGULAMENTUL DELEGAT AL COMISIEI de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei și de modificare a Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei

În anexă, se pune la dispoziția delegațiilor documentul C(2022) 4882 final - ANNEX.

Anexă: C(2022) 4882 final - ANNEX

COMISIA
EUROPEANĂ

Bruxelles, 14.7.2022
C(2022) 4882 final

ANNEX

ANEXĂ

la

REGULAMENTUL DELEGAT AL COMISIEI

de stabilire a normelor de aplicare a Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului în ceea ce privește cerințele referitoare la managementul riscurilor în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației impuse organizațiilor care intră sub incidența Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei și de modificare a Regulamentelor (UE) nr. 748/2012 și (UE) nr. 139/2014 ale Comisiei

ANEXĂ

SECURITATEA INFORMAȚIILOR – CERINȚE APLICABILE ORGANIZAȚIEI

[PARTEA-IS.D.OR]

IS.D.OR.100 Domeniul de aplicare

Prezenta parte stabilește cerințele care trebuie îndeplinite de organizațiile menționate la articolul 2 din prezentul regulament.

IS.D.OR.200 Sistemul de management al securității informațiilor (SMSI)

(a) Pentru a atinge obiectivele prevăzute la articolul 1, organizația trebuie să instituie, să implementeze și să mențină un sistem de management al securității informațiilor (SMSI) care asigură faptul că organizația:

(1) instituie o politică de securitate a informațiilor în care sunt prevăzute principiile generale ale organizației în ceea ce privește impactul potențial al riscurilor în materie de securitate a informațiilor asupra siguranței aviației;

(2) identifică și examinează riscurile în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.205;

(3) definește și implementează măsurile de tratare a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.210;

(4) implementează un sistem de raportare internă în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.215;

(5) definește și implementează, în conformitate cu punctul IS.D.OR.220, măsurile necesare pentru detectarea evenimentelor de securitate a informațiilor, le identifică pe cele care sunt considerate incidente cu impact potențial asupra siguranței aviației, cu excepția cazurilor permise conform punctului IS.D.OR.205 litera (e), asigură un răspuns la respectivele incidentele de securitate a informațiilor și se redresează în urma acestora;

(6) implementează măsurile care au fost notificate de autoritatea competentă ca reacție imediată la un incident sau o vulnerabilitate în materie de securitate a informațiilor cu impact asupra siguranței aviației;

(7) ia măsurile corespunzătoare, în conformitate cu punctul IS.D.OR.225, pentru abordarea constatărilor notificate de autoritatea competentă;

(8) implementează un sistem de raportare externă în conformitate cu punctul IS.D.OR.230, astfel încât autoritatea competentă să poată lua măsuri corespunzătoare;

(9) îndeplinește cerințele de la punctul IS.D.OR.235 când subcontractează altor organizații orice parte a activităților menționate la punctul IS.D.OR.200;

(10) îndeplinește cerințele în materie de personal stabilite la punctul IS.D.OR.240;

(11) îndeplinește cerințele de păstrare a evidențelor stabilite la punctul IS.D.OR.245;

(12) monitorizează îndeplinirea de către organizație a cerințelor din prezentul regulament și transmite managerului responsabil sau, în cazul organizațiilor de proiectare, șefului organizației de proiectare feedback cu privire la constatări, pentru a asigura implementarea efectivă a măsurilor corective;

(13) protejează, fără a aduce atingere cerințelor aplicabile în materie de raportare a incidentelor, confidențialitatea oricăror informații pe care organizația le-ar fi putut primi de la alte organizații, în funcție de nivelul de sensibilitate a informațiilor respective.

(b) Pentru a îndeplini în permanență cerințele menționate la articolul 1, organizația trebuie să implementeze un proces de îmbunătățire continuă în conformitate cu punctul IS.D.OR.260.

(c) Organizația trebuie să documenteze, în conformitate cu punctul IS.D.OR.250, toate procesele, procedurile, rolurile și responsabilitățile cheie necesare pentru a se conforma punctului IS.D.OR.200 litera (a) și să instituie un proces de modificare a documentației respective. Modificările aduse respectivelor procese, proceduri, roluri și responsabilități se gestionează în conformitate cu punctul IS.D.OR.255.

(d) Procesele, procedurile, rolurile și responsabilitățile instituite de organizație pentru a se conforma punctului IS.D.OR.200 litera (a) trebuie să corespundă naturii și complexității activităților sale, pe baza unei evaluări a riscurilor în materie de securitate a informațiilor inerente activităților respective, și pot fi integrate în alte sisteme de management existente care sunt deja implementate de organizație.

(e) Fără a se aduce atingere obligației de conformitate cu cerințele de raportare prevăzute în Regulamentul (UE) nr. 376/2014[1] și cu cerințele de la punctul IS.D.OR.200 litera (a) subpunctul (13), organizația poate primi din partea autorității competente aprobarea de a nu implementa cerințele menționate la literele (a)-(d) și cerințele conexe prevăzute la punctele IS.D.OR.205 – IS.D.OR.260, dacă demonstrează într-un mod considerat satisfăcător de autoritatea respectivă că activitățile, instalațiile și resursele sale, precum și serviciile pe care le operează, furnizează, primește și menține nu prezintă niciun risc în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației pentru organizația în sine sau pentru alte organizații. Aprobarea trebuie să se bazeze pe o evaluare documentată a riscurilor în materie de securitate a informațiilor, efectuată de organizație sau de o parte terță în conformitate cu punctul IS.D.OR.205 și examinată și aprobată de autoritatea sa competentă.

Menținerea valabilității respectivei aprobări va fi examinată de autoritatea competentă în urma ciclului de audit de supraveghere aplicabil și ori de câte ori sunt implementate modificări ale domeniului de activitate al organizației.

IS.D.OR.205 Evaluarea riscurilor în materie de securitate a informațiilor

(a) Organizația trebuie să identifice toate elementele sale care ar putea fi expuse unor riscuri în materie de securitate a informațiilor. Acestea trebuie să includă:

(1) activitățile, instalațiile și resursele organizației, precum și serviciile pe care le operează, furnizează, primește sau menține organizația;

(2) echipamentele, sistemele, datele și informațiile care contribuie la funcționarea elementelor enumerate la subpunctul (1).

(b) Organizația trebuie să identifice interfețele pe care le are cu alte organizații și care ar putea conduce la expunerea reciprocă la riscuri în materie de securitate a informațiilor.

(c) În ceea ce privește elementele și interfețele menționate la literele (a) și (b), organizația trebuie să identifice riscurile în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației. Pentru fiecare risc identificat, organizația trebuie:

(1) să atribuie un nivel de risc în conformitate cu o clasificare predefinită stabilită de organizație;

[1] Regulamentul (UE) nr. 376/2014 al Parlamentului European și al Consiliului din 3 aprilie 2014 privind raportarea, analiza și acțiunile subsecvente cu privire la evenimentele de aviație civilă, de modificare a Regulamentului (UE) nr. 996/2010 al Parlamentului European și al Consiliului și de abrogare a Directivei 2003/42/CE a Parlamentului European și a Consiliului, și a Regulamentelor (CE) nr. 1321/2007 și (CE) nr. 1330/2007 ale Comisiei (JO L 122, 24.4.2014, p. 18).

(2) să asocieze fiecare risc și nivelul său aferent cu elementul sau interfața corespunzătoare identificată în conformitate cu literele (a) și (b).

Clasificarea predefinită menționată la subpunctul (1) trebuie să țină seama de potențialul de producere a scenariului de amenințare și de gravitatea consecințelor acestuia asupra siguranței. Pe baza acestei clasificări și ținând cont dacă organizația dispune sau nu de un proces structurat și repetabil de management al riscurilor pentru operațiuni, organizația trebuie să fie în măsură să stabilească dacă riscul este acceptabil sau dacă trebuie tratat în conformitate cu punctul IS.D.OR.210.

Pentru a se facilita comparabilitatea reciprocă a evaluărilor riscurilor, la atribuirea nivelului de risc în temeiul subpunctului (1) se ține seama de informațiile relevante obținute în coordonare cu organizațiile menționate la litera (b).

(d) Organizația trebuie să revizuiască și să actualizeze evaluarea riscurilor efectuată în conformitate cu literele (a), (b) și (c) în oricare dintre următoarele situații:

(1) când există o modificare a elementelor expuse unor riscuri în materie de securitate a informațiilor;

(2) când există o modificare a interfețelor dintre organizație și alte organizații sau o modificare a riscurilor comunicate de celelalte organizații;

(3) când există o modificare a informațiilor sau a cunoștințelor utilizate pentru identificarea, analizarea și clasificarea riscurilor;

(4) analiza incidentelor de securitate a informațiilor a permis desprinderea de învățăminte.

IS.D.OR.210 Tratarea riscurilor în materie de securitate a informațiilor

(a) Organizația trebuie să elaboreze măsuri de abordare a riscurilor inacceptabile identificate în conformitate cu punctul IS.D.OR.205, să le implementeze în timp util și să verifice menținerea eficacității acestora. Respectivele măsuri trebuie să permită organizației:

(1) să controleze circumstanțele care contribuie la apariția efectivă a scenariului de amenințare;

(2) să diminueze consecințele asupra siguranței aviației, asociate materializării scenariului de amenințare;

(3) să evite riscurile.

Respectivele măsuri nu trebuie să introducă noi riscuri potențiale inacceptabile pentru siguranța aviației.

(b) Persoana menționată la punctul IS.D.OR.240 literele (a) și (b) și ceilalți membri vizați ai personalului organizației trebuie să fie informați de rezultatul evaluării riscurilor efectuate în conformitate cu punctul IS.D.OR.205, de scenariile de amenințare

corespunzătoare și de măsurile care trebuie implementate.

Organizația trebuie să informeze, de asemenea, organizațiile cu care are o interfață în conformitate cu punctul IS.D.OR.205 litera (b) cu privire la orice risc comun celor două organizații.

IS.D.OR.215 Sistemul de raportare internă în materie de securitate a informațiilor

(a) Organizația trebuie să instituie un sistem de raportare internă pentru a permite colectarea și evaluarea evenimentelor legate de securitatea informațiilor, inclusiv a celor care trebuie raportate în temeiul punctului IS.D.OR.230.

(b) Sistemul respectiv și procesul menționat la punctul IS.D.OR.220 trebuie să îi permită organizației:

(1) să identifice care dintre evenimentele raportate în temeiul literei (a) sunt considerate incidente de securitate a informațiilor sau vulnerabilități cu impact potențial asupra siguranței aviației;

(2) să identifice cauzele și factorii determinanți ai incidentelor de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu punctul (1) și să le abordeze în cadrul procesului de management al riscurilor în materie de securitate a informațiilor în conformitate cu punctele IS.D.OR.205 și IS.D.OR.220;

(3) să asigure o evaluare a tuturor informațiilor cunoscute și relevante legate de incidentele de securitate a informațiilor și vulnerabilitățile identificate în conformitate cu punctul (1);

(4) să asigure implementarea unei metode de distribuire internă a informațiilor, după caz.

(c) Orice organizație subcontractată care ar putea expune organizația la riscuri în materie de securitate a informațiilor cu impact potențial asupra siguranței aviației are obligația de a raporta organizației evenimentele de securitate a informațiilor. Rapoartele respective se transmit prin procedurile stabilite în angajamentele contractuale specifice și se evaluează în conformitate cu litera (b).

(d) Organizația trebuie să coopereze în cadrul investigațiilor cu orice altă organizație care are o contribuție semnificativă la securitatea informațiilor în cadrul propriilor sale activități.

(e) Organizația poate integra sistemul de raportare respectiv în alte sisteme de raportare pe care le-a implementat deja.

IS.D.OR.220 Incidentele de securitate a informațiilor – detectare, răspuns și redresare

(a) În funcție de rezultatul evaluării riscurilor, efectuată în conformitate cu punctul IS.D.OR.205, și de rezultatul tratării riscurilor, efectuată în conformitate cu punctul

IS.D.OR.210, organizația trebuie să implementeze măsuri de detectare a incidentelor și vulnerabilităților care indică materializarea potențială a unor riscuri inacceptabile și care pot avea un impact potențial asupra siguranței aviației. Respectivele măsuri de detectare trebuie să permită organizației:

(1) să identifice abaterile de la valorile de referință predeterminate ale performanței funcționale;

(2) să declanșeze avertizări pentru activarea unor măsuri de răspuns adecvate, în cazul oricărei abateri.

(b) Organizația trebuie să implementeze măsuri pentru a răspunde oricăror evenimente identificate în conformitate cu litera (a) care se pot transforma ori s-au transformat într-un incident de securitate a informațiilor. Aceste măsuri de răspuns trebuie să permită organizației:

(1) să declanșeze reacția la avertizările menționate la litera (a) subpunctul (2) prin activarea unor resurse și planuri de acțiune predefinite;

(2) să limiteze răspândirea unui atac și să evite materializarea deplină a unui scenariu de amenințare;

(3) să controleze modul de defectare al elementelor afectate definite la punctul IS.D.OR.205 litera (a).

(c) Organizația trebuie să implementeze măsuri de redresare în urma incidentelor de securitate a informațiilor, inclusiv măsuri de urgență, dacă este necesar. Respectivele măsuri de redresare trebuie să permită organizației:

(1) să elimine situația care a cauzat incidentul sau să o limiteze la un nivel tolerabil;

(2) să asigure atingerea unei stări de siguranță a elementelor afectate definite la punctul IS.D.OR.205 litera (a) în timpul de redresare definit în prealabil de organizație.

IS.D.OR.225 Răspunsul la constatările notificate de autoritatea competentă

(a) După primirea notificării constatărilor de la autoritatea competentă, organizația trebuie:

(1) să identifice atât cauza sau cauzele profunde ale apariției neconformității, cât și factorii care contribuie la aceasta;

2. să definească un plan de acțiuni corective;

3. să demonstreze corectarea neconformității într-un mod considerat satisfăcător de către autoritatea competentă.

(b) Acțiunile menționate la litera (a) trebuie întreprinse în termenul convenit cu autoritatea competentă.

IS.D.OR.230 Sistemul de raportare externă în materie de securitate a informațiilor

(a) Organizația trebuie să implementeze un sistem de raportare în materie de securitate a informațiilor care să fie conform cu cerințele stabilite în Regulamentul (UE) nr. 376/2014 și în actele delegate și de punere în aplicare ale acestuia, dacă regulamentul respectiv îi este aplicabil.

(b) Fără a aduce atingere obligațiilor prevăzute în Regulamentul (UE) nr. 376/2014, organizația trebuie să se asigure că orice incident de securitate a informațiilor sau vulnerabilitate care poate reprezenta un risc semnificativ pentru siguranța aviației este raportată autorității sale competente. În plus:

(1) atunci când un astfel de incident sau o astfel de vulnerabilitate afectează o aeronavă ori un sistem sau o componentă asociată, organizația trebuie să raporteze acest lucru și titularului aprobării de proiect;

(2) atunci când un astfel de incident sau o astfel de vulnerabilitate afectează un sistem sau element constitutiv utilizat de organizație, ea trebuie să raporteze acest lucru organizației responsabile cu proiectarea sistemului sau a elementului constitutiv.

(c) Organizația trebuie să raporteze situațiile menționate la litera (b) după cum urmează:

(1) se transmite o notificare autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, de îndată ce organizația ia cunoștință de situație;

(2) se transmite un raport autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv, cât mai curând posibil, însă fără a depăși 72 de ore de la momentul în care organizația a luat cunoștință de situație, în afara cazului în care circumstanțe excepționale împiedică acest lucru.

Raportul se întocmește în forma definită de autoritatea competentă și trebuie să conțină toate informațiile relevante despre situația de care a luat cunoștință organizația;

(3) se transmite autorității competente și, dacă este cazul, titularului aprobării de proiect sau organizației responsabile cu proiectarea sistemului sau a elementului constitutiv un raport de urmărire în care se oferă detalii privind acțiunile întreprinse sau pe care organizația intenționează să le întreprindă în urma incidentului, precum și privind acțiunile pe care organizația intenționează să le întreprindă pentru a preveni, în viitor, producerea unor incidente similare de securitate a informațiilor.

Raportul de urmărire se transmite de îndată ce au fost identificate respectivele acțiuni și se întocmește în forma definită de autoritatea competentă.

IS.D.OR.235 Subcontractarea activităților de management al securității informațiilor

(a) Organizația trebuie să se asigure că, atunci când subcontractează altor organizații orice parte a activităților menționate la punctul IS.D.OR.200, activitățile subcontractate respectă cerințele din prezentul regulament și că organizația subcontractată lucrează sub supravegherea sa. Organizația trebuie să se asigure că riscurile asociate activităților subcontractate sunt gestionate în mod corespunzător.

(b) Organizația trebuie să se asigure că autoritatea competentă poate avea acces, la cerere, la organizația subcontractată, pentru a determina menținerea conformității cu cerințele aplicabile stabilite în prezentul regulament.

IS.D.OR.240 Cerințele în materie de personal

(a) Managerul responsabil al organizației sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare, desemnat în conformitate cu Regulamentul (UE) nr. 748/2012 și cu Regulamentul (UE) nr. 139/2014, astfel cum se menționează la articolul 2 alineatul (1) literele (a) și (b) din prezentul regulament, trebuie să aibă drepturile statutare necesare pentru a se asigura că toate activitățile prevăzute în prezentul regulament pot fi finanțate și efectuate. Persoana respectivă trebuie:

(1) să se asigure că sunt disponibile toate resursele necesare pentru a se conforma cerințelor prezentului regulament;

(2) să stabilească și să promoveze politica de securitate a informațiilor menționată la punctul IS.D.OR.200 litera (a) subpunctul (1);

(3) să demonstreze că deține cunoștințe de bază privind prezentul regulament.

(b) Managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare trebuie să numească o persoană sau un grup de persoane pentru a asigura conformitatea organizației cu cerințele prezentului regulament și trebuie să definească nivelul de autoritate al acestora. Persoana sau grupul de persoane au obligația să raporteze direct managerului responsabil sau, în cazul organizațiilor de proiectare, șefului organizației de proiectare și trebuie să dețină pregătirea, cunoștințele și experiența necesare executării responsabilităților asumate. În cadrul procedurilor trebuie să se stabilească cine suplinește o anumită persoană în cazul unei absențe îndelungate a persoanei respective.

(c) Managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare trebuie să însărcineze o persoană sau un grup de persoane cu responsabilitatea de a gestiona funcția de monitorizare a conformității menționată la punctul IS.D.OR.200 litera (a) subpunctul 12.

(d) Atunci când organizația partajează structuri organizaționale, politici, procese și proceduri în materie de securitate a informațiilor cu alte organizații sau cu domenii ale propriei organizări care nu fac parte din aprobare sau din declarație, managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare, își poate delega activitățile unei persoane responsabile comune.

Într-un astfel de caz, se stabilesc măsuri de coordonare între managerul responsabil al organizației sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare și

persoana responsabilă comună pentru a se asigura integrarea adecvată a managementului securității informațiilor în cadrul organizației.

(e) Managerul responsabil sau șeful organizației de proiectare ori persoana responsabilă comună menționată la litera (d) trebuie să aibă drepturile statutare necesare pentru a institui și menține structurile organizaționale, politicile, procesele și procedurile necesare pentru implementarea punctului IS.D.OR.200.

(f) Organizația trebuie să dispună de un proces prin care să se asigure că are suficient personal disponibil pentru îndeplinirea activităților reglementate de prezenta anexă.

(g) Organizația trebuie să dispună de un proces prin care să se asigure că personalul menționat la litera (f) are competența necesară pentru a-și îndeplini sarcinile.

(h) Organizația trebuie să dispună de un proces prin care să se asigure că personalul este informat de responsabilitățile aferente rolurilor și sarcinilor atribuite.

(i) Organizația trebuie să se asigure că identitatea și fiabilitatea personalului care are acces la sistemele informatice și la datele care fac obiectul cerințelor prezentului regulament sunt stabilite în mod corespunzător.

IS.D.OR.245 Păstrarea evidențelor

(a) Organizația trebuie să păstreze evidența activităților sale de management al securității informațiilor.

(1) Organizația trebuie să se asigure că următoarele evidențe sunt arhivate și trasabile:

(i) orice aprobare primită și orice evaluare conexă a riscurilor în materie de securitate a informațiilor în conformitate cu punctul IS.D.OR.200 litera (e);

(ii) contractele pentru activitățile menționate la punctul IS.D.OR.200 litera (a) subpunctul (9);

(iii) evidențele proceselor-cheie menționate la punctul IS.D.OR.200 litera (d);

(iv) evidențele riscurilor identificate în evaluarea riscurilor menționată la punctul IS.D.OR.205, împreună cu măsurile conexe de tratare a riscurilor menționate la punctul IS.D.OR.210;

(v) evidențele incidentelor și vulnerabilităților în materie de securitate a informațiilor raportate în conformitate cu sistemele de raportare menționate la punctele IS.D.OR.215 și IS.D.OR.230;

(vi) evidențele evenimentelor de securitate a informațiilor care ar putea necesita o reevaluare în vederea depistării unor incidente sau vulnerabilități nedetectate în materie de securitate a informațiilor.

(2) Evidențele menționate la subpunctul (1) punctul (i) se păstrează timp de cel puțin cinci ani de la data la care aprobarea și-a pierdut valabilitatea.

(3) Evidențele menționate la subpunctul (1) punctul (ii) se păstrează timp de cel puțin cinci ani de la data la care contractul a fost modificat sau reziliat.

(4) Evidențele menționate la subpunctul (1) punctele (iii), (iv) și (v) se păstrează timp de cel puțin cinci ani.

(5) Evidențele menționate la subpunctul (1) punctul (vi) se păstrează până la reevaluarea respectivelor evenimente de securitate a informațiilor, efectuată cu o periodicitate definită în cadrul unei proceduri instituite de organizație.

(b) Organizația trebuie să păstreze evidența calificărilor și a experienței personalului propriu implicat în activități de management al securității informațiilor.

(1) Evidențele calificărilor și experienței personalului se păstrează atât timp cât persoana lucrează pentru organizație și timp de cel puțin trei ani după ce persoana a părăsit organizația.

(2) Membrii personalului trebuie să primească, la cerere, acces la evidențele personale. În plus, la cererea membrilor personalului, organizația trebuie să le furnizeze acestora, la părăsirea organizației, o copie a evidențelor personale.

(c) Formatul evidențelor se specifică în procedurile organizației.

(d) Evidențele se stochează astfel încât să fie protejate împotriva deteriorării, alterării și furtului, informațiile fiind identificate, după caz, conform nivelului lor de clasificare de securitate. Organizația trebuie să se asigure că evidențele sunt stocate prin mijloace care să asigure integritatea, autenticitatea și accesul autorizat.

IS.D.OR.250 Manualul de management al securității informațiilor (MMSI)

(a) Organizația trebuie să pună la dispoziția autorității competente un manual de management al securității informațiilor (MMSI) și, când este cazul, eventualele manuale și proceduri conexe la care se face trimitere în manualul respectiv, conținând:

(1) o declarație semnată de managerul responsabil sau, în cazul organizațiilor de proiectare, de șeful organizației de proiectare, prin care se confirmă că organizația își va desfășura în permanență activitatea în conformitate cu prezenta anexă și cu MMSI. Dacă managerul responsabil sau, în cazul organizațiilor de proiectare, șeful organizației de proiectare nu este directorul general al organizației, declarația trebuie să fie contrasemnată de directorul general;

(2) funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei sau persoanelor menționate la punctul IS.D.OR.240 literele (b) și (c);

(3) funcția, numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanei responsabile comune menționate la punctul IS.D.OR.240 litera (d), dacă este cazul;

(4) politica de securitate a informațiilor instituită de organizație, astfel cum este menționată la punctul IS.D.OR.200 litera (a) subpunctul (1);

(5) o descriere generală a resurselor umane, din punctul de vedere al efectivelor și categoriilor, precum și a sistemului instituit pentru planificarea disponibilității personalului, astfel cum se prevede la punctul IS.D.OR.240 litera (d);

(6) funcția (funcțiile), numele, atribuțiile, răspunderile, responsabilitățile și competențele persoanelor-cheie responsabile cu implementarea punctului IS.D.OR.200, inclusiv ale persoanei sau persoanelor responsabile cu funcția de monitorizare a conformității, menționată la punctul IS.D.OR.200 litera (a) subpunctul (12);

(7) o organigramă ilustrând liniile ierarhice conexe în materie de răspundere și responsabilitate pentru persoanele menționate la subpunctele (2) și (6);

(8) descrierea sistemului de raportare internă menționat la punctul IS.D.OR.215;

(9) procedurile în care se specifică modul în care organizația asigură conformitatea cu prezenta parte, în particular:

(i) documentația menționată la punctul IS.D.OR.200 litera (c);

(ii) procedurile care definesc modul în care organizația controlează eventualele activități subcontractate, astfel cum se menționează la punctul IS.D.OR.200 litera (a) subpunctul (9);

(iii) procedura de modificare a MMSI-ului, definită la litera (c);

(10) informații detaliate referitoare la mijloace de conformare alternative aprobate în prezent.

(b) Ediția inițială a MMSI-ului trebuie să fie aprobată, iar o copie trebuie să fie păstrată de autoritatea competentă. MMSI-ul trebuie modificat în funcție de necesități, astfel încât să reprezinte o descriere actualizată a SMSI-ului organizației. O copie a oricăror modificări aduse MMSI-ului trebuie transmisă autorității competente.

(c) Modificările aduse MMSI-ului se gestionează în cadrul unei proceduri instituite de organizație. Orice modificare care nu este acoperită de domeniul de aplicare al acestei proceduri și orice modificare legată de modificările menționate la punctul IS.D.OR.255 litera (b) trebuie să fie aprobată de autoritatea competentă.

(d) Organizația poate integra MMSI-ul în alte specificații sau manuale de management pe care le deține, cu condiția să existe o referință încrucișată clară indicând părțile din specificațiile sau manualul de management care corespund diferitelor cerințe cuprinse în prezenta anexă.

IS.D.OR.255 Modificări ale sistemului de management al securității informațiilor

(a) Modificările aduse SMSI-ului pot fi gestionate și notificate autorității competente în cadrul unei proceduri elaborate de organizație. Procedură respectivă trebuie să fie aprobată de autoritatea competentă.

(b) În ceea ce privește modificările SMSI-ului care nu fac obiectul procedurii menționate la litera (a), organizația trebuie să solicite și să obțină o aprobare din partea autorității competente.

În ceea ce privește aceste modificări:

(1) cererea se depune înainte să intervină modificarea respectivă, pentru a i se permite autorității competente să stabilească continuitatea conformității cu prezentul regulament și să modifice, dacă este necesar, certificatul organizației și condițiile de aprobare anexate acestuia.

(2) organizația trebuie să pună la dispoziția autorității competente toate informațiile solicitate pentru evaluarea modificării;

(3) modificarea se implementează numai după primirea unei aprobări oficiale din partea autorității competente;

(4) organizația trebuie să își desfășoare activitatea în condițiile stabilite de autoritatea competentă în timpul implementării modificărilor respective.

IS.D.OR.260 Îmbunătățirea continuă

(a) Organizația trebuie să evalueze, cu ajutorul unor indicatori de performanță adecvați, eficacitatea și maturitatea SMSI-ului. Respectiva evaluare trebuie efectuată pe baza unui calendar predefinit de organizație sau în urma unui incident de securitate a informațiilor.

(b) Dacă în urma evaluării efectuate în conformitate cu litera (a) se constată deficiențe, organizația trebuie să ia măsurile de îmbunătățire necesare pentru a se asigura că SMSI-ul continuă să se conformeze cerințelor aplicabile și că el menține riscurile în materie de securitate a informațiilor la un nivel acceptabil. În plus, organizația trebuie să reevalueze elementele SMSI vizate de măsurile adoptate.