GHID DE ÎNDRUMARE

a implementării activităților desfășurate de către entități în aplicarea Normei privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de Autoritatea de Supraveghere Financiară

I. Domeniul de aplicare

Prezentul ghid de îndrumare cuprinde detalii și parametrii, în conformitate cu prevederile art.7 alin. (2) din Norma A.S.F. nr. 6/2015 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de Autoritatea de Supraveghere Financiară, referitoare la modalitatea de implementare corespunzătoare a activităților desfășurate de către entități în aplicarea acesteia.

Prezentul ghid stabilește modul în care este aplicată Norma A.S.F. nr. 6/2015 cu privire la practicile adecvate referitoare la activitățile desfășurate de către entitățile reglementate, autorizate/avizate și supravegheate de A.S.F., așa cum sunt acestea prevăzute în anexa nr.2 a acestei norme.

Aceste ghiduri se referă la următoarele activități:

A. Evaluarea internă a riscului operațional și registrul riscurilor
B. Organizarea pe procese a activităților aferente utilizării tehnologiei informației:
    1. Managementul disponibilității;
    2. Managementul utilizatorilor;
    3. Managementul incidentelor;
    4. Managementul schimbării;
    5. Managementul capacității;
    6. Managementul configurațiilor;
    7. Managementul nivelurilor de servicii;
    8. Managementul securității;
    9. Managementul continuității.
C. Punctele de control și măsurare:
    1. Controale generale;
    2. Controale la nivelul programelor informatice;
    3. Controale de flux financiar.
D. Elementele de control tip indicatori de performanță (KPI) pe procese
E. Indicatorii cheie de risc (KRI) aferenți punctelor de control
F. Managementul Securităţii Sistemelor Informatice și de Comunicaţii:
    1. Măsuri organizatorice;
    2. Proceduri de securitate;
    3. Evaluarea internă de securitate;
    4. Plan de cooperare în domeniul securității sistemelor și a informației.

II. Modalitatea de aplicare

Entitățile reglementate, autorizate/avizate şi supravegheate de A.S.F. vor încorpora prezentele ghiduri în activitatea lor curentă, în funcție de categoria de risc în care sunt încadrate conform Normei A.S.F. nr. 6/2015 și în conformitate cu natura, dimensiunea şi complexitatea activităților desfășurate.

III. Ghiduri de implementare

A. Evaluarea internă a riscurilor operaţionale și registrul riscurilor

A.1) Entităţile îşi evaluează intern riscurile operaţionale generate de utilizarea tehnologiei informaţiilor şi comunicaţiilor şi constituie un Registru al riscurilor operaţionale generate de utilizarea sistemelor informatice de către oameni, procese, sisteme şi mediul extern.
A.2) Entităţile identifică toate categoriile relevante de risc, le menţionează în registrul riscurilor pe patru categorii: oameni, procese, sisteme/tehnologii şi mediul extern, ţinând cont de riscurile activităţilor externalizate către furnizorii de produse şi servicii informatice şi de comunicaţii.
A.3) Evaluarea de risc se efectuează regulat, dar cel puţin anual. Funcţia de administrare a riscului integrează toate riscurile semnificative pentru entitate pe o hartă ce reprezintă profilul de risc al entității. Profilul de risc este analizat şi discutat oricând au loc schimbări importante în entitate.
A.4) A.S.F. va publica, pana la data de 30 iunie 2015, un exemplu de metodologie privind evaluarea interna a riscurilor care va propune și o metodă de calcul aferentă evaluării riscurilor, precum și un șablon pentru raportarea anuală a evaluării interne a riscurilor.

B. Organizarea pe procese a activităților aferente utilizării tehnologiei informației

1) Managementul disponibilității

B.1.1) Entităţile implementează un proces documentat de management al disponibilității în vederea asigurării funcționării sistemelor informatice pentru asigurarea serviciilor contractate de către clienți și a raportărilor către A.S.F.
Activitățile aferente procesului managementului disponibilității definesc, analizează, planifică, măsoară și îmbunătățesc aspectele legate de disponibilitatea unui serviciu IT.
B.1.2) Entitățile definesc nivelurile corespunzătoare referitoare la disponibilitatea serviciilor IT (interne sau externalizate), inclusiv a centrelor de procesare și stocare date. Entitățile utilizează centre de date pentru a asigura un timp corespunzător de funcţionare raportat la durata unui an calendaristic echivalent unui centru de date de nivel 2.
B.1.3) Entitățile contractează servicii cu furnizori de soluții informatice care implementează cel puțin standardul SR ISO/IEC 27001, precum și cerințele prevăzute la art. 11alin. (1) din Norma A.S.F. nr. 6/2015. În cazul externalizărilor în lanț, cerințele trebuie să fie îndeplinite de toți furnizorii pe lanțul externalizării.

2) Managementul utilizatorilor

B.2.1) Entităţile implementează un proces de instruire pentru utilizatorii sistemelor informatice, astfel:

1. *instruirea utilizatorilor* - înstruirea individuală cu privire la utilizarea sistemelor informatice este obligatorie şi trebuie să se facă ţinând cont de responsabilităţile specifice fiecărui utilizator;
2. *instruirea noilor angajați* - noii angajaţi trebuie să fie instruiți obligatoriu cu privire la utilizarea sistemelor informatice în momentul angajării. Angajații vor semna un document prin care să se confirme faptul că au luat la cunoştinţă politica de securitate a entității;
3. *instruirea pentru sistemele noi introduse* - entitatile se angajează să instruiască toţi utilizatorii sistemelor nou introduse pentru a garanta faptul că acestea vor fi folosite eficient şi că nu vor compromite securitatea informatică

B.2.2) Fiecare utilizator trebuie să aibă un identificator unic şi o parolă personală secretă pentru accesul la sistemele/programele informatice ale entității. Modul de selectare, folosire şi protecţie a parolelor, ca mecanism principal de control al accesului, trebuie să se facă în conformitate cu o politica de securitate internă. Accesul la sistemele proprii trebuie autorizat de către proprietarii

sistemelor, iar acest lucrul include drepturile de acces (sau privilegiile) acordate care trebuie înregistrate în Listele de Control a Accesului (Access Control List). Toate privilegiile de acces la sistemele informatice trebuie revocate imediat în momentul în care un angajat îşi încetează activitatea în cadrul organizaţiei.

B.2.3) Privilegiile acordate utilizatorilor trebuie revizuite periodic pentru a determina dacă acestea continuă să fie necesare pentru ca utilizatorul să-şi poată îndeplini sarcinile ce îi revin. Dacă nu, aceste privilegii trebuie revocate imediat. Pentru orice conexiuni la distanta se va impune o durata maxima de viata a conexiunii inactive.

B.2.4) Modulele de conectare în sistem trebuie configurate astfel încât să limiteze numărul de încercări de conectare nereuşite înainte de a bloca accesul pentru utilizatorul respectiv. Pentru deblocarea accesului, utilizatorul trebuie să ia legătura personal cu administratorul de sistem.

B.2.5) Entitățile dispun de mecanisme privind gestionarea adecvată a accesului la sistemele/programele informatice importante, care vor ține cont cel puțin de următoarele:

1. Aplicaţiile din producţie la care au acces mai mulţi utilizatori trebuie să dispună de o politică de control a accesului;
2. Controlul accesului la aplicaţii trebuie configurat astfel încât să minimizeze riscurile cu privire la securitatea informaţiei şi să permită desfăşurarea în bune condiţii a activităţilor din cadrul organizatiei;
3. Utilizatorilor li se va permite accesul numai la comenzile şi funcţiile sistem pe care au dreptul să le folosească;
4. Accesul la informaţiile cu caracter personal trebuie permis numai angajaţilor care au nevoie de acest lucru pentru îndeplinirea sarcinilor ce le revin;
5. Accesul la sisteme trebuie jurnalizat şi monitorizat pentru a putea identifica acţiunile de folosire necorespunzătoare a acestora. Toate sistemele de calcul din producţie trebuie să dispună de jurnale de audit care să înregistreze cel puţin activităţile desfăşurate pe parcursul unei sesiuni utilizator: ID-ul utilizatorului, data şi timpul conectării în sistem, data şi timpul deconectării, aplicaţiile apelate, modificările efectuate asupra fişierelor critice din sistem, adăugarea sau modificarea de privilegii ale utilizatorului, precum şi momentele în care sistemul a fost pornit sau oprit.

B.2.6) Sistemele de calcul ce manipulează informaţii confidentiale trebuie să jurnalizeze toate evenimentele relevante din punct de vedere al securităţii cum ar fi: încercările de conectare la sistem, încercările de a folosi privilegii neautorizate, modificarea privilegiilor utilizatorilor, modificarea aplicaţiilor software din producţie şi modificarea software-ului de sistem.

B.2.7) Securitatea jurnalelor trebuie să fie suficient de ridicată pentru a evita dezactivarea, modificarea, ştergerea sau suprascrierea acestora. Accesul la jurnale trebuie permis numai persoanelor autorizate.

3) Managementul incidentelor

B.3.1) Entităţile implementează un proces documentat de management al incidentelor în vederea identificarii, colectării, analizării şi rezolvării incidentelor care afectează buna funcţionare a activității personalului propriu, a sistemelor informatice și de comunicații, a asigurării serviciilor către clienți, a raportărilor către A.S.F..

4) Managementul schimbării

B.4.1) Entităţile implementează un proces documentat de management al schimbării în vederea asigurării controlului asupra implementării modificărilor/schimbărilor solicitate de planurile de afaceri și operaționale, la nivelul organizației, al personalului, al proceselor, al sistemelor, al

serviciilor IT și al operării cu furnizorii externi. Entităţile implementează procesul de management al schimbării printre altele pentru asigurarea trasabilității, transparenței, documentării și evidenței, a reducerii erorilor și fraudelor.
B.4.2) Entităţile implementează schimbări adaptând, după caz, bunele practici aferente managementului de proiecte.

a) Managementul ciclului de viață al programelor informatice

B.4.3) Entităţile implementează un proces documentat de colectare a cerințelor de afaceri, de analizare a lor, de redactare a specificațiilor de afaceri și tehnice, de alocare a resurselor, de dezvoltare software a programului informatic, de testare, promovare, de suport după implementare și de primire de noi cerințe pentru modificarea celor inițiale după ce acestea sunt deja în funcțiune.

b) Managementul versiunilor

B.4.4) Entităţile păstrează istoricul cu privire la procesul de versionare a aplicaţiilor/sistemelor în scopul normei, pe toată perioada de utilizare a aplicației/sistemului. În acest sens:

1) fiecare versiune a unui program informatic va primi un cod unic;
2) testele de acceptanță sunt finalizate si semnate de utilizatorii de test și de utilizatorii finali;
3) toate versiunile trebuie aprobate înaintea implementării.

c) Managementul testării și asigurării calității programelor informatice

B.4.5) Entităţile testează sistemul informatic utilizat cu resurse umane și tehnice interne sau externe entităţii.

B.4.6) Testarea se efectuează în baza unei proceduri scrise și a unui scenariu formalizat de testare, prin care să se asigure că testarea răspunde cerinţelor impuse la managementul securităţii.

5) Managementul capacității

B.5.1) Entităţile implementează un proces documentat privind asigurarea performanței, scalabilității și a capacității serviciilor IT asigurate de infrastructura informatică pentru prevenirea afectării parțiale sau totale a capacității de procesare, stocare sau furnizare a serviciilor către beneficiari sau a raportărilor către A.S.F..

6) Managementul configurațiilor

B.6.1) Entităţile implementează un proces documentat pentru evidența activelor tangibile și intangibile informatice și de comunicații, inclusiv utilizatori, manuale de utilizare si documentații ale programelor informatice.

7) Managementul nivelurilor de servicii

B.7.1) Entităţile implementează un proces documentat privind definirea nivelurilor agreate de servicii aferente furnizorilor de servicii externalizate.
B.7.2) Entităţile identifică și aplică măsuri de securitate pentru gestionarea accesului furnizorilor la mijloacele de procesare a datelor și la informaţii.
B.7.3) Entităţile prevăd în contractul cu furnizorului extern:

1) responsabilități și obligaţii legale;
2) cerinţele de securitate sau măsurile interne de securitate necesare;

3) responsabilități şi obligaţii aferente accesării, procesării sau gestionării informaţiilor entității şi a facilităţilor sale de procesare a datelor;
4) responsabilități şi obligaţii de planificare a perioadei de tranziţie şi rezolvarea problemelor potenţiale ale întreruperii operaţiunilor pe parcursul acestei perioade;
5) planificări pentru situaţii neprevăzute;
6) culegerea de informaţii şi monitorizarea privind incidentele de securitate şi managementul acestora;
7) planificarea şi gestionarea tranziţiei spre un acord de servicii IT externalizate şi aplică procese adecvate pentru managementul schimbării şi renegocierea/rezilierea acordurilor.

B.7.4) Acordul de servicii externalizate prevede procedurile pentru continuarea procesării în cazul în care furnizorul devine incapabil să mai furnizeze serviciile, pentru a se evita întârzierea nejustificată în obţinerea unor servicii înlocuitoare.

B.7.5) Acordurile de servicii externalizate pot implica şi alte părţi. Acordurile care oferă acces unei terţe părţi trebuie să includă posibilitatea de desemnare explicită a acestora, criteriile precum şi condiţiile pentru accesul şi implicarea acestora.

8) Managementul securităţii

a) Cerințe generale

B.8.1)Entitățile implementează cerințele generale de securitate astfel cum sunt prevăzute la art. 8 alin. (1) din Norma A.S.F. nr. 6/2015.

B.8.2)De asemenea, entitățile urmăresc:(i) păstrarea la sediul propriu a documentaţiei complete şi actualizate, pe fiecare nivel de acces, a programelor informatice utilizate;(ii) respectarea oricăror altor cerinţe care rezultă din dispoziţiile legale în vigoare, aplicabile în funcţie de obiectul de activitate al entităţii;

b) Teste de penetrare

B.8.3)Entitățile adoptă măsuri pentru implementarea unui proces de testare a posibilității de penetrare a sistemelor, cel puțin din exteriorul entității, la nivel de program informatic, sisteme de operare, baze de date, rețea.

9) Managementul continuității

B.9.1) Entitățile asigură replicarea datelor și a sistemelor informatice importante. Pentru sistemele informatice importante, entitățile urmăresc să asigure:
a) o disponibilitate ridicată, corelată cu natura, dimensiunea și complexitatea activității, la sediul principal de procesare a entității (propriu sau externalizat);
b) un sistem de recuperare în caz de dezastru situat fie într-o altă locaţie a entităţii, fie prin intermediul unui furnizor extern de servicii, care să minimizeze riscul de dezastru natural;
c) furnizorul extern de servicii trebuie să respecte cerințele de la managementul disponibilității prevăzute la cap. B.1.2)
B.9.2) Funcţionarea planurilor alternative de recuperare și continuitate a afacerii se testează periodic pe baza unor scenarii practice și reale, cu asigurarea posibilității continuării operaţiunilor pe sistemele de rezervă.
B.9.3) Entitățile își continuă activitatea în caz de avarie sau dezastru, prin intermediul unui centru de recuperare cu reluarea activității într-un interval de timp foarte scurt, definit în cadrul profilului de risc. Pentru entitățile încadrate în categoria de risc major intervalul de timp optim

este de două ore. Pentru entitățile încadrate în categoria de risc important intervalul de timp optim este de două zile. Pentru entitățile încadrate în categoria de risc mediu intervalul de timp optim este de patru zile. Pentru entitățile încadrate în categoria de risc scăzut intervalul de timp optim este de cinci zile.

B.9.4) Entitățile urmăresc următoarele caracteristici ale centrului de date și ale planului de recuperare:

a) este permanent operațional, pe perioada de definire a serviciilor (număr zile pe săptămână, număr ore pe zi) și asigură serviciile IT susținute de sistemele informatice importante și definite în planul de recuperare, în timpul angajat prin registrul riscurilor și comunicat către A.S.F.;

b) este sincronizat cu sistemul principal pentru a se asigura același nivel sau un nivel de servicii cu o scădere acceptabilă de servicii pentru serviciile replicate;

c) asigură comutarea și continuarea activității în locația alternativă, în intervalul de timp prevăzut în profilul de risc al entității, evaluat și comunicat către A.S.F. Entitățile urmăresc încadrarea în intervalul de timp optim prevăzut la pct. B. 8.3).

B.9.5) Entitățile definesc un proces de control al incidentului în cadrul planului de continuare a activității, prin intermediul unui plan de urgență pentru administrarea situației de criză.

C) Puncte de control și măsurare

C.1) Entitățile implementează următoarele tipuri de controaleca urmare a evaluărilor proprii și, când este cazul:

a) controale preventive;
b) controale de avertizare.

C.2) Entitățile controlează riscurile generate de utilizarea sistemelor informatice prin:

a) stabilirea de obiective de control;

b) implementarea de puncte de control de către entitate sau de furnizorul extern de servicii;

c) monitorizarea punctelor de control și a indicatorilor cheie de risc.

În acest scop, se implementează atât controale generale la nivelul sistemului informatic, cât şi controale specifice la nivelul fiecărei componente a acestuia, după caz. Informaţiile din punctele de control vor fi colectate periodic la alegerea entității sau când este cazul și vor fi păstrate la dispoziţia entității și raportate către A.S.F. pe baza cerințelor de raportare.

C.3) Entitățile aplică proceduri operaționale în domeniul combaterii spălării banilor și finanțării terorismului, precum și regimului de sancțiuni internaționale ca parte integrată a reglementărilor emise de A.S.F..

a) Controale generale

Controalele generale la nivelul entităţilor sau al furnizorilor externi de servicii sunt proiectate încât informaţiile financiare generate de sistemele informatice ale entității să fie de încredere, reale și corecte. Controalele generale includ:

a) controale referitoare la sincronizarea de timp la o referință recunoscută naţional sau internaţional;
b) controale asupra operării centrului de date;
c) controale asupra sistemelor de aplicaţii;
d) controale asupra securităţii accesului;
e) controale asupra dezvoltării, administrării şi întreţinerii programelor informatice.

Controalele generale includ şi verificarea existenţei şi aplicării unei strategii de informatizare, a politicilor de aprobare și efectuare a achiziţiilor, a externalizărilor serviciilor informatice, inclusiv prevenirea riscului sistemic datorat criminalităţii informatice.

b) Controale programe informatice

Entitățile implementează controale la nivelul programelor informatice prin proceduri de validare şi control incluse în codul software utilizat, prin includerea punctelor de control în codul software pentru prevenirea și detectarea tranzacţiilor neautorizate, precum și proceduri manuale de verificare a modului de procesare a tranzacţiilor şi a efectuării operaţiunilor.

Entitățile implementează controale aferente separării mediului de dezvoltare a programelor informatice de mediul de testare a programelor informatice și de mediul de operare a programelor informatice. Accesul la diversele medii trebuie controlat, ţinând cont de exigenţa limitării riscurilor şi a fraudei. Controalele susțin siguranţa datelor și a informațiilor, separarea de atribuții în funcție de cele trei tipuri de medii, limitând accesul persoanelor neautorizate la informații și în mediul de operare şi înregistrând toate tentativele de acces neautorizate.
Entitățile asigură siguranţa fizică a sistemelor hardware, software şi a bazelor de date, pentru prevenirea utilizării necorespunzătoare a informaţiei de către personalul entității în vederea obţinerii unor beneficii personale sau prejudicierea reputaţiei societăţii.

Entitățile se asigură că furnizorii de programe informatice dezvoltate la cerere de către entități utilizează obiectivele de control recomandate de bunele practici în domeniu pentru controalele aferente programelor informatice.

c) Controale de flux financiar

Entitățile implementează controale de flux financiar pentru verificarea periodică, din perspectiva procesării electronice, a fluxurile de date dintre datele din contabilitate, datele din activitățile operaționale, datele de la parteneri.

D) Elemente de control tip indicatori de performanță (KPI) pe procese

Entitățile selecționează și monitorizează indicatorii cheie de performanță (KPI) pe care îi consideră relevanți pentru procesele proprii.

E) Indicatori cheie de risc (KRI) aferenți punctelor de control

E.1) Entitățile urmăresc riscurile operaționale din perspectiva expunerii și a schimbărilor în profilul de risc operațional prin indicatori de risc în funcție de natura, dimensiunea și complexitatea activității. Entitățile își definesc apetitului la risc prin definirea unor limite la care indicatorii de risc sunt folosiți ca suport. Entitățile asigură procesul de monitorizare și măsură prin indicatorii cheie de risc (KRI), identificând pierderile operaționale potențiale cauzate de deficiențele legate de IT și comunicații.
E.2) Entitățile își stabilesc un set de indicatori cheie de risc (KRI) aferenți proceselor specificate în Norma A.S.F. nr. 6/2015, în conformitate cu categoria proprie de risc.

F) Managementul Securităţii Sistemelor Informatice și de Comunicaţii

Entităţile care utilizează sisteme informatice de prelucrare automată a datelor vor elabora un set de măsuri de siguranţă, în concordanţă cu legislaţia în domeniu, utilizând principiile referențialului SR ISO/CEI 27002 (fără a se solicita certificarea expresă), în funcție de profilul și apetitul de risc, natura, dimensiunea și complexitatea activităţii entității și de categoria de risc alocată de către A.S.F. sau a solicitării exprese a A.S.F. către o entitate specifică, ce va include cel puţin următoarele elemente:

1. Măsuri organizatorice

(1) Entitățile definesc și implementează următoarelor activități, proceduri și responsabilități:

a) politica de securitate;

b) obiectivele de securitate;

c) desemnarea responsabilului cu securitatea informaţiei;

d) desemnarea în cadrul entităţii a personalului responsabil cu:

(i) intervenţia în caz de incidente;

(ii) mentenanţa programelor informatice şi a echipamentelor;

(iii) recuperarea datelor în caz de dezastre;

(iv) formularea propunerilor privind modificarea regulamentelor interioare şi a procedurilor de lucru, astfel încât să se asigure îndeplinirea obiectivelor de securitate.

(2) Entităţile se înregistrează obligatoriu ca operatori de date cu caracter personal conform legii.

(3) Entităţile instruiesc periodic personalul angajat, inclusiv angajaţii cheie, în vederea cunoașterii riscurilor generale și specifice generate de oameni, procese, sisteme și mediul extern, riscurile aferente criminalității și a obligațiilor ce decurg din setul de măsuri prevăzut în prezentul ghid.

2. Proceduri de securitate

(1) Entitățile dețin proceduri de securitate care descriu activitățile sau procesele specificate în Norma A.S.F. nr. 6/2015, conform încadrării în categoria de risc, care se desfăşoară la nivelul tuturor departamentelor.

(2) Toate documentele referitoare la procedurile de sistem vor face parte integrantă din procedurile de securitate.

3. Evaluarea internă de securitate

Entitățile evaluează intern anual, sau de câte ori este nevoie, rezultatele sistemului de securitate, revizia rezultatelor și acțiunile corective pentru determinarea nivelului de maturitate internă a controalelor de securitate ale entității, conform tabelului de mai jos, care este parte integrantă din evaluarea internă a riscurilor entității respective.

Evaluare internă a maturității controalelor de securitate

Domenii ale Securității Informației	Ratingul maturității controalelor de securitate					
	0 - Ne existent	1 - Inițial / Ad-Hoc	2 - Repetabil dar intuitiv	3 - Proces definit	4 - Controlat și măsurabil	5 - Optimizat
I. Politici de securitate	Nu au fost stabilite politici prin care să se definească securitatea informațională	Politicile și procedurile nu au fost formalizate	Au fost definite obiective, dar acestea nu sunt clare si concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurate de entitate	Personalul responsabil a fost informat si instruit cu privire la politicile si obiectivele stabilite	Se aplică proceduri de verificare a realizării obiectivelor stabilite prin politici	Politicile corespund exigentelor sporite, sunt revizuite periodic, inclusiv in cazul aparitiei riscurilor semnificative
II. Securitatea organizațională	Nu au fost definite principiile care stau la baza managementului securității	Există principii la nivel informal	Au fost definite principii, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Intreg personalul responsabil a fost informat si instruit in legatura cu principiile aprobate de conducere	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
III. Controlul și clasificarea activelor	Nu au fost definite proceduri de securitate și	Procedurile de securitate și siguranță a activelor sunt	A fost stabilita modalitatea de control, dar acestea nu se efectueaza in mod concret	Persoanele responsabile au fost informate in raport cu	Persoanele responsabile aplică adecvat procedurile de	Procedurile de securitate și siguranță a activelor sunt

Domenii ale Securității Informației	Ratingul maturității controalelor de securitate					
	0 - Ne existent	1 - Inițial / Ad-Hoc	2 - Repetabil dar intuitiv	3 - Proces definit	4 - Controlat și măsurabil	5 - Optimizat
	siguranță a activelor	aplicate informal		procedurile de securitate și siguranță a activelor	securitate și siguranță a activelor	revizuite și modificate periodic, inclusiv in cazul aparitiei riscurilor semnificative
IV. Securitatea personalului	Nu au fost definite principiile care stau la baza managementului securității si incidentelor	Există principii la doar la nivel informal	Au fost definite principii, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra principiilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
V. Securitatea fizica și de mediului de lucru	Nu au fost definite planuri/ proceduri de securiate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite periodic, si sunt avute in vedere concluziile controalelor generale implementate in cadrul entitatilor
VI. Securitatea echipamentelor	Nu au fost definite planuri/ proceduri de securiate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
VII. Controale generale	Nu au fost definite controalele generale pentru gestionarea activității	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare stabilite si aprobate de conducere, se respecta indicatiile privind controalele generale	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
VIII. Managementul operațiunilor și a comunicațiilor	Nu au fost definite obiectivele specifice	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
IX. Controlul accesului	Nu au fost definite controalele pentru verificarea accesului	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Principiile care guvernează accesul securizat la informații au fost aduse la cunostinta personalului responsabil, care a fost instruit in consecinta	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
X. Întreținerea și dezvoltarea sistemelor	Nu au fost definite instrumente și proceduri	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Au fost respectate cerintele legate de securitate ce trebuie avute in vedere in fiecare etapa a ciclului de viata a sistemelor	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative

Domenii ale Securității Informației	Ratingul maturității controalelor de securitate					
	0 - Ne existent	1 - Inițial / Ad-Hoc	2 - Repetabil dar intuitiv	3 - Proces definit	4 - Controlat și măsurabil	5 - Optimizat
XI. Continuitatea afacerii	Nu au fost definite controalele de management al continuitatii	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative
XII. Conformitate	Nu au fost definite controalele privind asigurarea conformității	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, dupa caz, nu sunt aplicabile in raport activitatea propriu-zisa desfasurata de entitate	Asupra procedurilor aprobate de conducere a fost informat si instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si imbunatatite periodic, inclusiv in cazul aparitiei riscurilor semnificative

4. Plan de cooperare

a) Entităţile cooperează în cadrul unui Plan de cooperare în domeniul securității sistemelor și a informației care va fi stabilit de către A.S.F. șitransmit date și informații relevante în acest sens privind amenințările, vulnerabilităţile şi incidentele generatoare de riscuri majore și crize, proprii sau ale furnizorilor externi, inclusiv cele de securitate cibernetică, tehnici şi tehnologii folosite în rezolvarea incidentelor/crizelor, precum şi bune practici pentru protecţia infrastructurilor proprii, inclusiv cibernetice.

b) Entităţile participă, la solicitarea A.S.F., și susțin schimbul de informaţii anonimizate dintre diverse echipe de răspuns la situații de urgență, precum echipele tip CERT, utilizatori, autorităţi, producători de echipamente şi soluţii de securitate cibernetică, precum şi furnizori de servicii informatice și comunicații.

c) Entităţile înființează puncte de contact pentru colectarea sesizărilor şi a informaţiilor despre incidente de securitate atât automatizat, cât şi prin comunicare directă securizată, după caz.