GHID DE ÎNDRUMARE
a implementării activităților desfășurate de către entități în aplicarea Normei nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entităţile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară

CUPRINS

I. Domeniul de aplicare

Prezentul ghid de îndrumare este adoptat în conformitate cu prevederile art.15 alin. (5) din Norma nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară, și cuprinde orientări referitoare la modalitatea de implementare corespunzătoare a activităților desfășurate de către entități în aplicarea acesteia.

Orientările din prezentul ghid pot să fie considerate ca practici adecvate referitoare la activitățile desfășurate de către entitățile reglementate, autorizate/avizate și/sau supravegheate de A.S.F., așa cum sunt acestea prevăzute în anexa nr.2 a Normei nr. 4/2018. Cu toate acestea, entitățile, pe baza unei fundamentări adecvate, pot să aplice practici echivalente sau să implementeze standarde ori bune practici care sunt la un nivel superior orientărilor din prezentul ghid de îndrumare.

Aceste orientări 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.

Termenii şi expresiile utilizate în prezentul ghid au semnificaţia prevăzută în legislaţia specifică sectoarelor de supraveghere financiară, precum şi semnificaţiile următoarele:

1. acord de furnizare a serviciului la parametrii agreaţi (SLA) - un acord între un furnizor de servicii IT şi un client, care descrie unul sau mai multe servicii IT, documentează nivelurile de serviciu ţintă agreate şi specifică obligaţiile furnizorului de servicii IT şi ale clientului;
2. activităţi de control informatic - politici, proceduri şi practici aplicate pentru atingerea obiectivelor entităţii şi pentru îndeplinirea strategiilor de eliminare a riscurilor, concepute pentru atingerea fiecărui obiectiv de control pentru eliminarea riscului identificat;
3. ameninţări - capacităţi, strategii, intenţii sau planuri ce periclitează infrastructurile, materializate prin atitudini, gesturi, acte sau fapte cu impact asupra securităţii activităţii entităţilor şi a integrităţii sectorului în care activează;

4. angajaţi/persoane-cheie - persoane cu funcţii de conducere/persoane relevante/persoane semnificative care au atribuţii şi răspunderi cu privire la planificarea, conducerea şi controlarea activităţilor entităţii;
5. bune practici - activităţi sau procese certificate care au fost folosite cu succes în mai multe organizaţii şi au căpătat o largă recunoaştere, precum SR ISO/IEC 27002, ISO 20.002, cadrul de lucru şi metodologiile ISACA - COBIT, RiskIT, dar fără a se limita la acestea;
6. centrul principal de date - centru de date care asigură serviciile IT şi procesează în mod curent datele, tranzacţiile şi operaţiunile entităţii;
7. CERT/Echipă sau centru de răspuns la incidente de urgenţă aferente securităţii informatice - structură organizaţională specializată în vederea colectării, analizării, identificării, prevenirii şi reacţiei la incidente cibernetice cu impact semnificativ;
8. COBIT/Obiective de Control pentru Tehnologia Informaţiilor şi Tehnologii Conexe - furnizează îndrumare şi bună practică pentru managementul controalelor proceselor IT, fiind publicat de către ISACA în colaborare cu IT Governance Institute (ITGI);
9. factori de risc - situaţii, împrejurări, elemente, condiţii sau conjuncturi interne şi externe, uneori dublate şi de acţiune, ce determină ori favorizează materializarea unei ameninţări la adresa infrastructurilor importante, în funcţie de o vulnerabilitate determinată, generând efecte de insecuritate;
10. infrastructură esenţială/critică - un sistem informatic sau o componentă a acestuia, care este esenţial pentru menţinerea funcţiilor infrastructurii financiare, a căror perturbare afectează semnificativ buna funcţionare a acesteia, cu un impact semnificativ ca urmare a incapacităţii de a menţine respectivele funcţii;
11. infrastructură importantă - sistem informatic propriu sau externalizat, care asigură funcţionarea activităţilor şi serviciilor principale ale entităţii;
12. internet - reţea internaţională de calculatoare, formată prin interconectarea reţelelor globale (Wide Area Network - WAN) independente (particulare, comerciale, academice sau guvernamentale), destinată facilitării schimbului de date şi informaţii între utilizatori;
13. SR ISO/IEC 27002 - cod de practică internaţională pentru managementul securităţii informaţiei, având specificaţia SR ISO/IEC 27001;
14. ISO/IEC 20000 - standard care stabileşte cerinţele pentru un sistem de management al serviciilor IT, bazat pe setul de publicaţii de bune practici al Bibliotecii pentru Infrastructura IT/IT Infrastructure Library - ITIL;
15. obiectiv de control (informatic) - scop şi mijloc care se reflectă în punctele de control din care se extrag indicatori-cheie de risc;
16. persoane - investitori, brokeri de asigurare, agenţi de asigurare, furnizori externi de servicii, alţi terţi sau colaboratori ai entităţii, angajaţi proprii - pe perioadă nedeterminată, respectiv determinată; participanţi la fondurile de pensii private. Entităţile vor raporta defalcat pe fiecare tip de "persoane" în funcţie de specificul activităţii proprii;
17. portofolii, tranzacţii şi active - conturile proprii ale investitorilor pe piaţa de capital sau ale clienţilor societăţilor de asigurări; portofolii de investitori, asiguraţi, operaţiuni cu activele investitorilor, activele proprii ale intermediarului şi/sau ale persoanelor relevante;
18. soluţie informatică - un produs de tip sistem informatic, o combinaţie de produse sau o combinaţie de produse şi servicii informatice care sunt furnizate de un producător sau furnizor de servicii informatice sau de comunicaţii.

II. Modalitatea de aplicare

Entitățile reglementate, autorizate/avizate și/sau supravegheate de A.S.F. vor încorpora prezentele orientări în activitatea lor curentă, în funcție de activitățile obligatorii corespunzătoare fiecărei categorii de risc în care sunt încadrate conform Normei nr. 4/2018 și în conformitate cu natura, dimensiunea și complexitatea activităților desfășurate.

III. Ghiduri de implementare

A. Evaluarea internă a riscurilor operaţionale şi registrul riscurilor

A.1) Entităţile își evaluează intern riscurile operaţionale generate de utilizarea tehnologiei informaţiilor și comunicaţiilor și constituie un Registru al riscurilor operaţionale generate de utilizarea sistemelor informatice.

A.2) Entitățile identifică toate categoriile relevante de risc, le menționează în registrul riscurilor pe patru categorii: oameni, procese, sisteme/tehnologii și mediul extern, ținând cont de riscurile activităților externalizate către furnizorii de produse şi servicii informatice și de comunicaţii.

A.3) Evaluarea de risc se efectuează regulat, dar cel puţin anual. Funcția 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 de conducerea superioară oricând au loc schimbări importante în entitate.

A.4) A.S.F. publică, un exemplu de metodologie privind evaluarea interna a riscurilor, inclusiv un exemplu de metodă de calcul aferentă evaluării riscurilor, precum și un șablon orientativ pentru raportarea anuală a evaluării interne a riscurilor.

A.5) Exemplul de metodologie și șablonul pentru raportarea anuală menționate la pct. A.4) pot să fie ajustate de fiecare entitate în funcție de natura, dimensiunea și complexitatea activității acesteia, precum și în funcție de gradul de maturitate al acesteia.

B. Organizarea pe procese a activităţilor aferente utilizării tehnologiei informaţiei

1. Managementul disponibilității

B.1.1) Entităţile implementează un proces documentat de management al disponibilității în vederea asigurării funcționării sistemelor informatice pentru asigurarea serviciilor oferite 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, cel puțin, 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. 46 alin. (1) din Norma nr. 4/2018. În cazul externalizărilor în lanț, cerințele sunt 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* - instruirea individuală cu privire la utilizarea sistemelor informatice trebuie să se facă ţinând cont de responsabilităţile specifice fiecărui utilizator;
2. *instruirea noilor angajaţi* - noii angajaţi sunt instruiţi 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* - entitățile se angajează să instruiască toţi utilizatorii sistemelor nou introduse pentru a se asigura de faptul că acestea vor fi folosite eficient şi că nu vor compromite securitatea informatică.

B.2.2) Fiecare utilizator are 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, se face în conformitate cu o politica de securitate internă. Accesul la sistemele proprii este autorizat de către proprietarii sistemelor, iar acest lucru include drepturile de acces (sau privilegiile) acordate care sunt apoi înregistrate în Listele de Control a Accesului (Access Control List). Toate privilegiile de acces la sistemele informatice sunt revocate imediat,după ce un angajat îşi încetează activitatea în cadrul entității.

B.2.3) Privilegiile acordate utilizatorilor sunt 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 sunt revocate imediat. Pentru orice conexiuni la distanta se stabilește și implementează o durata maxima de viață a conexiunii inactive.

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

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

1. Aplicaţiile din producţie la care au acces mai mulţi utilizatori dispun de o politică de control a accesului;
2. Controlul accesului la aplicaţii este configurat astfel încât să minimizeze riscurile cu privire la securitatea informaţiei şi să permită desfăşurarea în bune condiţii a activităţilor din cadrul entității;
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 este permis numai angajaţilor care au nevoie de acest lucru pentru îndeplinirea sarcinilor ce le revin;
5. Accesul la sisteme este jurnalizat şi monitorizat pentru a putea identifica acţiunile de

folosire necorespunzătoare a acestora. Toate sistemele de calcul din producţie dispun de jurnale de audit care înregistrează cel puţin activităţile desfăşurate pe parcursul unei sesiuni de utilizator, astfel: ID-ul utilizatorului, data şi ora conectării în sistem, data şi ora 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 confidențiale jurnalizează 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 este suficient de ridicată pentru a evita dezactivarea, modificarea, ştergerea sau suprascrierea acestora. Accesul la jurnale este permis numai persoanelor autorizate.

3. Managementul incidentelor

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

B.3.2) Planul de răspuns la incidentele de securitate informatică, prevăzut la art. 17 din Norma nr. 4/2018 poate să fie de sine stătător ori poate fi inclus în planul de recuperare în caz de dezastru sau în planul de continuitatea afacerii.

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 entității, 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 nr. 4/2018, pe toată perioada de utilizare a aplicației/sistemului. În acest sens se ține cont cel puțin de următoarele:

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 (se va indica numele şi funcţia persoanelor care au calitatea de a aproba implementarea versiunii, precum şi documentul semnat şi datat prin care au fost aprobate).
4. în documentaţia aferentă fiecărei versiuni se vor preciza motivele care au stat la baza elaborării acesteia, precum şi documentul semnat şi datat prin care a fost aprobată.

c) Managementul testării și asigurării calității programelor informatice

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

B.4.6) Testarea se efectuează în baza unei proceduri scrise și a unui scenariu formalizat de testare, prin care să se asigure, cel puțin, că testarea răspunde cerinţelor impuse la managementul securității (se indică numele şi funcţia persoanelor care au calitatea de a aproba procedura şi scenariul de testare, precum şi documentul semnat şi datat prin care au fost aprobate).

5. Managementul capacității

B.5.1) Entităţile implementează un proces documentat privind asigurarea performanței, scalabilității și a capacității serviciilor IT asigurate de infrastructura informatică, cel puțin, 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, cel puțin pentru 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 şi 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 cel puțin următoarele:
1. responsabilități şi 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 și monitorizarea privind incidentele de securitate şi managementul acestora;
7. planificarea şi gestionarea tranziţiei spre un acord de servicii IT externalizate şi aplicarea de procese adecvate pentru managementul schimbării şi renegocierea/rezilierea acordurilor.

B.7.4) Acordul de servicii externalizate prevede, cel puțin, 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 includ, cel puțin, 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. 16 alin. (1) din Norma nr. 4/2018.

B.8.2) De asemenea, entitățile urmăresc cel puțin:

1. păstrarea la sediul propriu a documentaţiei complete și actualizate, pe fiecare nivel de acces, a programelor informatice utilizate;
2. 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 testarea securității aplicațiilor incluse în scopul auditului, testarea securității sistemelor de operare utilizate în cadrul entității și testarea securității infrastructurii rețelei, precum și testarea vulnerabilităților identificate în urma scanării de securitate, 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, urmărind să asigure cel puțin:

1. o disponibilitate ridicată, corelată cu natura, dimensiunea și complexitatea activității, la sediul principal de procesare a entității (propriu sau externalizat);
2. 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;
3. respectarea cerințelor de la managementul disponibilității prevăzute la pct. B.1.2) de către furnizorul extern de servicii.

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 de conducerea superioară a fiecărei entități, urmărindu-se atingerea următoarelor ținte:

1. pentru entitățile încadrate în categoria de risc major intervalul de timp optim să fie de două ore.
2. pentru entitățile încadrate în categoria de risc important intervalul de timp optim să fie de două zile.
3. pentru entitățile încadrate în categoria de risc mediu intervalul de timp optim să fie de patru zile.

4. pentru entitățile încadrate în categoria de risc scăzut intervalul de timp optim să fie de cinci zile.

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

1. 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 stabilit de conducerea superioară a fiecărei entități;
2. 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;
3. asigură comutarea și continuarea activității în locația alternativă, în intervalul de timp stabilit de conducerea superioară a fiecărei entități. Entitățile urmăresc, de regulă, încadrarea în intervalul de timp optim prevăzut la pct. B. 9.3).

B.9.5) Entitățile definesc un proces de control al incidentelor 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 controale ca urmare a evaluărilor proprii și, când este cazul:

1. controale preventive;
2. controale de avertizare.

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

1. stabilirea de obiective de control;
2. implementarea de puncte de control de către entitate sau de furnizorul extern de servicii;
3. 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. la solicitarea autorității.

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..

1. Controale generale

C.4) Controalele generale la nivelul entităţilor sau al furnizorilor externi de servicii sunt proiectate astfel încât informaţiile financiare generate de sistemele informatice ale entității să fie de încredere, reale și corecte. Controalele generale includ:

1. controale referitoare la sincronizarea de timp la o referință recunoscută naţional sau internaţional;
2. controale asupra operării centrului de date;
3. controale asupra sistemelor de aplicaţii;
4. controale asupra securității accesului;
5. controale asupra dezvoltării, administrării și întreţinerii programelor informatice.

C.5) 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.

2. Controale programe informatice

C.6) Entitățile implementează controale la nivelul programelor informatice, cel puțin, 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 prin proceduri manuale de verificare a modului de procesare a tranzacţiilor şi a efectuării operaţiunilor.

C.7) Entitățile implementează controale aferente separării mediului de dezvoltare a programelor informatice de mediul de testare a programelor informatice, de mediul de operare și producție al acestora. Accesul la diversele medii este 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 şi înregistrând toate tentativele de acces neautorizate.

C.8) 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.

C.9) 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.

3. Controale de flux financiar

C.10) 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 și datele de la parteneri.

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

D.1) 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 activităţii. Entitățile își definesc toleranța 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 nr. 4/2018, în conformitate cu categoria proprie de risc.

F) Managementul Securităţii Sistemelor Informatice şi de Comunicaţii

F.1) Entităţile care utilizează sisteme informatice de prelucrare automată a datelor vor elabora, cel puțin, 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 toleranța la risc, natura, dimensiunea și complexitatea activităţii entității și de categoria de risc a acesteia.

1. Măsuri organizatorice

F.2.1) Entitățile definesc și implementează, cel puțin, următoarele activități, proceduri și responsabilități:

1. politica de securitate;
2. obiectivele de securitate;
3. desemnarea responsabilului cu securitatea informaţiei;
4. desemnarea în cadrul entităţii a personalului responsabil cu:
   i. intervenţia în caz de incidente informatice;
   ii. mentenanţa programelor informatice şi a echipamentelor;
   iii. recuperarea datelor în caz de dezastru;
   iv. formularea propunerilor privind modificarea regulamentelor interioare şi a procedurilor de lucru, astfel încât să se asigure îndeplinirea obiectivelor de securitate.

F.2.2) Entităţile care procesează date cu caracter personal se înregistrează ca operatori de date cu caracter personal conform legii.

F.2.3) Entităţile instruiesc periodic personalul angajat, inclusiv angajaţii cheie, în vederea cunoaşterii riscurilor operaționale, riscurile aferente criminalității și a obligaţiilor ce decurg din setul de măsuri recomandate în prezentul ghid.

2. Proceduri de securitate

F.3.1) Entitățile dețin proceduri de securitate care descriu, cel puțin, activitățile sau procesele specificate în Norma nr. 4/2018, conform încadrării în categoria de risc, care se desfăşoară la nivelul tuturor structurilor organizatorice.

F.3.2) Toate documentele referitoare la procedurile de sistem vor face parte integrantă din procedurile de securitate.

3. Evaluarea internă de securitate

F.4) 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 și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată 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 apariției riscurilor

Domenii ale Securității	Ratingul maturității controalelor de securitate					
						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, după caz, nu sunt aplicabile în raport activitatea propriu-zisă cu desfășurată de entitate	Întreg personalul responsabil a fost informat si instruit în legătura cu principiile aprobate de conducere	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si îmbunătățite periodic, inclusiv in cazul apariției riscurilor semnificative
III. Controlul și clasificarea activelor	Nu au fost definite proceduri de securitate și siguranță a activelor	Procedurile de securitate și siguranță a activelor sunt aplicate informal	A fost stabilita modalitatea de control, dar acestea nu se efectuează în mod concret	Persoanele responsabile au fost informate in raport cu procedurile de securitate și siguranță a activelor	Persoanele responsabile aplică adecvat procedurile de securitate și siguranță a activelor	Procedurile de securitate și siguranță a activelor sunt revizuite și modificate periodic, inclusiv in cazul apariției riscurilor semnificative
IV. Securitatea personalului	Nu au fost definite principiile care stau la baza managementului securității si incidentelor	Există principii doar la nivel informal	Au fost definite principii, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată 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 îmbunătățite periodic, inclusiv in cazul apariției riscurilor semnificative
V. Securitatea fizica și de mediului de lucru	Nu au fost definite planuri/ proceduri de securitate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite periodic, si sunt avute în vedere concluziile controalelor generale implementate in cadrul entităților
VI. Securitatea echipamentelor	Nu au fost definite planuri/ proceduri de securitate	Există politici si proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite si îmbunătățite periodic, inclusiv in cazul apariției 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, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare stabilite si aprobate de conducere, se respectă indicațiile privind controalele generale	Procedurile sunt revizuite și îmbunătățite periodic, inclusiv în cazul apariției riscurilor semnificative
VIII. Managementul operațiunilor și a comunicațiilor	Nu au fost definite obiectivele specifice	Există politici și proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite și îmbunătățite periodic, inclusiv în cazul apariției riscurilor semnificative
IX. Controlul accesului	Nu au fost definite controalele pentru verificarea accesului	Există politici și proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Principiile care guvernează accesul securizat la informații au fost aduse la cunoștința personalului responsabil, care a fost instruit în consecința	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate de conducere	Procedurile sunt revizuite și îmbunătățite periodic, inclusiv în cazul apariției riscurilor semnificative
X. Întreținerea	Nu au fost definite	Există politici și proceduri	Au fost definite proceduri, dar acestea nu sunt clare și	Asupra procedurilor	Au fost respectate	Procedurile sunt revizuite și

Domenii ale Securității	Ratingul maturității controalelor de securitate					
și dezvoltarea sistemelor	instrumente și proceduri	doar la nivel informal	concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	aprobate de conducere a fost informat și instruit întreg personalul responsabil	cerințele legate de securitate ce trebuie avute în vedere în fiecare etapă a ciclului de viață a sistemelor	îmbunătățite periodic, inclusiv în cazul apariției riscurilor semnificative
XI. Continuitatea afacerii	Nu au fost definite controalele de management al continuității	Există politici și proceduri doar la nivel informal	Au fost definite proceduri, dar acestea nu sunt clare și concise sau, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite și îmbunătățite periodic, inclusiv în cazul apariției 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, după caz, nu sunt aplicabile în raport cu activitatea propriu-zisă desfășurată de entitate	Asupra procedurilor aprobate de conducere a fost informat și instruit întreg personalul responsabil	Se aplică proceduri de verificare a respectării principiilor stabilite și aprobate	Procedurile sunt revizuite și îmbunătățite periodic, inclusiv în cazul apariției riscurilor semnificative

4. Plan de cooperare

F.5.1) Entităţile cooperează în cadrul unui Plan de cooperare în domeniul securității sistemelor și a informației care va fi stabilit de către A.S.F. și transmit 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, tehnicile şi tehnologiile folosite în rezolvarea incidentelor/crizelor, precum şi bune practici pentru protecţia infrastructurilor proprii, inclusiv cibernetice.

F.5.2) 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.

F.5.3) 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.