Norma nr. 4/2018 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară

În temeiul prevederilor art. 3 alin. (1) lit. b), art. 5, art. 6 alin. (2) şi ale art. 14 din Ordonanţa de urgenţă a Guvernului nr. 93/2012 privind înfiinţarea, organizarea şi funcţionarea Autorităţii de Supraveghere Financiară, aprobată cu modificări şi completări prin Legea nr. 113/2013, cu modificările şi completările ulterioare,

în urma deliberărilor Consiliului Autorităţii de Supraveghere Financiară din cadrul şedinţei din data de 28 februarie 2018,

Autoritatea de Supraveghere Financiară emite prezenta normă.

CAPITOLUL I
Dispoziţii generale

Art. 1. - (1) Prezenta normă stabileşte cerinţele la nivelul entităţilor autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară, denumită în continuare A.S.F., pentru identificarea, prevenirea şi reducerea impactului potenţial negativ al riscurilor operaţionale generate de utilizarea tehnologiei informaţiei şi comunicaţiilor la nivel de oameni, procese, sisteme şi mediu extern, inclusiv pentru fapte ce ţin de criminalitatea informatică.

(2) Prezenta normă reglementează activităţile şi operaţiunile pentru evaluarea, supravegherea şi controlul riscurilor operaţionale generate de utilizarea sistemelor informatice, precum şi gestionarea riscurilor privind securitatea sistemelor informatice importante în vederea asigurării securităţii informatice a entităţilor prevăzute la alin. (1).

Art. 2. - Prezenta normă se aplică următoarelor categorii de entităţi autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către A.S.F., denumite în continuare entităţi:

a) operatori de piaţă/operatori de sistem;

b) societăţi de administrare a investiţiilor (S.A.I.), administratori de fonduri de investiţii alternative (A.F.I.A.), respectiv:

1. societăţi care deţin active nete în portofoliu/administrate în valoare totală, cumulată pentru toate fondurile administrate, de peste 250 milioane euro, echivalent lei;

2. societăţi care deţin active nete în portofoliu/administrate în valoare totală, cumulată pentru toate fondurile administrate, de până la 250 milioane euro, echivalent lei;

c) depozitari centrali, case de compensare/contrapărţi centrale;

d) intermediari - societăţi de servicii de investiţii financiare (S.S.I.F.), sucursale ale intermediarilor din state terţe şi instituţii de credit din România autorizate de Banca Naţională a României în conformitate cu legislaţia bancară şi înscrise în Registrul A.S.F. în calitate de intermediar, respectiv:

1. intermediari care au calitatea de operatori independenţi;

2. S.S.I.F. semnificative din punctul de vedere al mărimii, organizării interne şi naturii, extinderii şi complexităţii activităţii, conform reglementărilor specifice;

3. intermediari care prestează servicii conexe de păstrare în siguranţă şi administrare a instrumentelor financiare în contul clienţilor, inclusiv custodia şi servicii în legătură cu aceasta, cum ar fi administrarea fondurilor sau garanţiilor;

4. intermediari care folosesc facilităţi de tranzacţionare prin internet (ADP/AS) - platforme de preluare şi transmitere a ordinelor clienţilor;

5. intermediari care au calitatea de market makeri şi/sau furnizori de lichiditate;

6. intermediari care tranzacţionează pe cont propriu şi nu se încadrează în categoriile de la pct. 1-5;

7. intermediari care nu tranzacţionează pe cont propriu şi nu se încadrează în categoriile de la pct. 1-5;

e) «abrogat»

f) Fondul de compensare a investitorilor, Fondul de garantare a asiguraţilor şi Fondul de garantare a drepturilor din sistemul de pensii private;

g) societăţi de asigurare şi reasigurare;

h) intermediari principali care desfăşoară activitate de distribuţie a produselor de asigurare şi reasigurare;

i) Biroul asigurătorilor de autovehicule din România;

j) entităţi care desfăşoară activitatea de depozitare a activelor organismelor de plasament colectiv şi a fondurilor de pensii private;

k) administratorii fondurilor de pensii private.

Art. 3. - (1) Entităţile prevăzute la art. 2 au obligaţia de a identifica toate sistemele informatice importante utilizate pe ambele componente, respectiv infrastructura hardware şi software, care sunt esenţiale în activitatea desfăşurată de către acestea.

(2) Sistemele informatice importante prevăzute la alin. (1) cuprind, în funcţie de tipul entităţii, cel puţin următoarele, fără a se limita la acestea:

a) sisteme informatice necesare pentru derularea în bune condiţii a activităţii autorizate/avizate de A.S.F.:

1. sisteme de tranzacţionare/sisteme alternative de tranzacţionare;

2. sisteme de compensare, decontare, depozitare şi custodie;

3. platforme/aplicaţii de tranzacţionare sau distribuţie prin internet sau telefon;

4. sisteme de gestiune asiguraţi;

5. sisteme de gestiune şi subscriere contracte de asigurare;

6. sisteme de înregistrare şi gestiune a dosarelor de daună;

7. platforme de emitere a contractelor de asigurare;

8. sisteme de calcul al comisioanelor;

9. sisteme de gestiune a contractelor de reasigurare;

10. sisteme de gestiune a participanţilor la fondurile de pensii private;

11. sisteme de administrare a portofoliilor de instrumente financiare ale fondurilor de pensii private;

12. sisteme de call-center;

13. aplicaţii online utilizate în scopul de distribuţie şi informare a clienţilor, precum accesarea conturilor online;

14. sisteme informatice de back-office, altele decât cele care se încadrează la pct. 1-13;

b) sisteme interne pentru asigurarea raportărilor către A.S.F. şi alte instituţii/entităţi ale pieţei financiare;

c) sisteme informatice folosite în activitatea financiar- contabilă a entităţii, cum ar fi programele de contabilitate;

d) sisteme electronice de vot şi alte sisteme informatice cu implicaţii semnificative asupra sistemului de guvernanţă al entităţii, precum sisteme de tip teleconferinţă/videoconferinţă utilizate pentru desfăşurarea la distanţă a şedinţelor consiliului de administraţie/consiliului de supraveghere;

e) sisteme informatice cu impact asupra planului pentru continuitatea afacerii şi redresării activităţii în caz de dezastre;

f) aplicaţii centrale de business, altele decât cele care se încadrează la lit. a)-e);

g) infrastructura informatică utilizată pentru sistemele informatice importante găzduite în locaţiile de centre de date.

(3) Entităţile au obligaţia să întocmească şi să actualizeze permanent un registru cu sistemele informatice importante identificate în conformitate cu prevederile alin. (1) şi (2).

(4) Registrul întocmit în conformitate cu prevederile alin. (3) este supus verificării de către auditorul IT.

Art. 4. - Entităţile extind scopul auditului IT şi la alte sisteme în situaţiile prevăzute la art. 29 alin. (1).

Art. 5. - (1) Prevederile prezentei norme se aplică de către entităţi în funcţie de categoria de risc stabilită de către A.S.F. conform prevederilor art. 10 şi 11, precum şi în funcţie de rezultatul evaluării interne a riscurilor, pe baza celor mai bune practici în domeniu.

(2) Categoria de risc corespunzătoare fiecărui tip de entitate este stabilită de către A.S.F. în funcţie de natura, dimensiunea şi complexitatea activităţii acesteia, precum şi de riscurile pe care le poate induce şi care au impact asupra activităţii.

Art. 6. - (1) Entităţile au obligaţia să evalueze anual şi să monitorizeze continuu riscurile operaţionale generate de utilizarea sistemelor informatice importante, să prioritizeze resursele, să implementeze măsuri de securitate informatică şi să monitorizeze eficacitatea acestora prin aplicarea managementului de risc.

(2) Modalitatea de implementare a măsurilor de securitate informatică prevăzute la alin. (1) este stabilită de fiecare entitate, în funcţie de profilul de risc, de riscurile identificate, de incidentele apărute, în conformitate cu cerinţele legale aplicabile.

Art. 7. - Entităţile participă la colectarea, analizarea, monitorizarea şi raportarea evenimentelor de securitate informatică, în cadrul sistemului care va fi dezvoltat de către A.S.F.

Art. 8. - Termenii şi expresiile utilizate în prezenta normă au înţelesul prevăzut în anexa nr. 1.

CAPITOLUL II
Încadrarea entităţilor în categorii de risc

Art. 9. - În scopul prezentei norme, fiecare entitate prevăzută la art. 2 se încadrează în una dintre următoarele categorii de risc:

a) risc major;

b) risc important;

c) risc mediu;

d) risc scăzut.

Art. 10. - Încadrarea entităţilor prevăzute la art. 2 lit. a) -j) în categoriile de risc menţionate la art. 9 este următoarea:

a) în categoria de risc major se încadrează entităţile prevăzute la art. 2 lit. a), lit. c), lit. d) pct. 1 şi lit. i);

b) în categoria de risc important se încadrează entităţile prevăzute la art. 2. lit. d) pct. 2, 4 şi 5, lit. g) şi j);

c) în categoria de risc mediu se încadrează entităţile prevăzute la art. 2 lit. b) pct. 1, lit. d) pct. 3 şi pct. 6 şi lit. f);

d) în categoria de risc scăzut se încadrează entităţile prevăzute la art. 2 lit. b) pct. 2, lit. d) pct. 7 şi lit. h).

Art. 11. - Încadrarea entităţilor prevăzute la art. 2 lit. k) se realizează individual în categoriile de risc prevăzute la art. 9, conform prevederilor art. 44 alin. (4) lit. e) şi ale art. 51 din Norma Autorităţii de Supraveghere Financiară nr. 3/2014 privind controlul intern, auditul intern şi administrarea riscurilor în sistemul de pensii private.

Art. 12. - Încadrarea, respectiv reîncadrarea entităţilor menţionate la art. 2 lit. b) se realizează în luna ianuarie a fiecărui an calendaristic, în baza valorii totale a activelor nete în portofoliu/administrate din ultima zi lucrătoare a anului anterior.

Art. 13. - Încadrarea, respectiv reîncadrarea entităţilor menţionate la art. 2 lit. d) se realizează în luna ianuarie a fiecărui an calendaristic, în baza activităţii autorizate de către A.S.F şi a deţinerii calităţii de market maker/furnizor de lichiditate în ultima zi lucrătoare a anului anterior.

Art. 14. - Entitatea care prestează mai multe tipuri de activităţi autorizate de către A.S.F. şi se încadrează în mai multe categorii de risc dintre cele prevăzute la art. 9 respectă obligaţiile pentru categoria de risc cea mai ridicată instituită de prezenta normă.

CAPITOLUL III

Dispoziţii privind activităţile obligatorii desfăşurate de către entităţi

Art. 15. - (1) Entităţile au obligaţia să desfăşoare cel puţin activităţile obligatorii corespunzătoare fiecărei categorii de risc prevăzute la art. 9, conform tabelului din anexa nr. 2.

(2) Entităţile au obligaţia ca, anual, să efectueze o scanare de vulnerabilităţi.

(3) Testele de penetrare regăsite în tabelul din anexa nr. 2 la lit. B) pct. 8 lit. c) au drept obiectiv testarea securităţii aplicaţiilor incluse în scopul auditului, testarea securităţii sistemelor de operare utilizate în cadrul entităţii şi testarea securităţii infrastructurii reţelei, precum şi testarea vulnerabilităţilor identificate în urma scanării de securitate.

(4) Entităţile au obligaţia să se asigure că în perioada supusă auditului IT sunt efectuate teste de penetrare externe, teste de penetrare interne şi teste de inginerie socială, fără a se limita la acestea.

(5) A.S.F. publică pe site-ul propriu un ghid de îndrumare care cuprinde detalii şi parametri privind modalitatea de implementare a activităţilor obligatorii prevăzute la alin. (1). Ghidul are un caracter orientativ şi poate fi actualizat de către A.S.F. în funcţie de bunele practici în domeniu.

Art. 16. - (1) Raportat la activitatea desfăşurată, entităţile au obligaţia să se asigure că sistemele informatice importante utilizate îndeplinesc cel puţin următoarele cerinţe:

a) asigură integritatea, confidenţialitatea, autenticitatea, disponibilitatea datelor în concordanţă cu categoria de risc a sistemului informatic important definită intern de către entitate, precum şi prelucrarea acestora în conformitate cu reglementările A.S.F., luând în considerare posibilitatea actualizării acestora în funcţie de modificările intervenite în legislaţia incidentă;

b) asigură respectarea conţinutului de informaţii prevăzut în formularele de raportare, aşa cum sunt prevăzute în legislaţia specifică, precum şi alte raportări solicitate prin reglementările A.S.F.;

c) asigură stocarea şi păstrarea datelor înregistrate şi jurnalizate de către sistemele de tranzacţionare, de emitere contracte de asigurări/avizare dosare de daune şi sisteme back- office pentru o perioadă de timp în conformitate cu legislaţia aplicabilă în vigoare. Sistemul de păstrare a datelor trebuie să permită ca aceste date să poată fi transmise sau puse la dispoziţia A.S.F. la cerere;

d) asigură elemente de identificare a datelor supuse prelucrării sau verificării, respectiv identificarea exactă a timpului la care au fost efectuate înregistrările şi identificarea utilizatorilor sistemului în acel moment;

e) asigură confidenţialitatea şi protecţia informaţiilor şi a programelor prin parole, coduri de identificare pentru accesul la informaţii, precum şi realizarea de copii de siguranţă pentru programele şi informaţiile deţinute;

f) asigură mecanisme de securitate şi control al sistemelor informatice importante, pentru păstrarea în siguranţă a datelor şi informaţiilor stocate, a fişierelor şi bazelor de date, inclusiv în situaţia unor incidente;

g) asigură reconstituirea rapoartelor şi informaţiilor supuse verificării;

h) asigură posibilitatea de restaurare a datelor arhivate pe suport digital extern, precum, dar fără a se limita la, informaţii, date introduse, situaţii financiare.

(2) Entităţile au obligaţia să se asigure că sunt îndeplinite următoarele cerinţe:

a) nu există posibilitatea autentificării multiple a mai multor persoane pe acelaşi cont de aplicaţie;

b) nedivulgarea credenţialelor, a parolelor sau a oricărui alt sistem de autentificare de către utilizatorii acestora;

c) utilizarea de credenţiale personalizate doar pentru personalul autorizat/înregistrat;

d) jurnalizarea, monitorizarea şi arhivarea în conformitate cu reglementările specifice în materie pentru a asigura controlul asupra accesului utilizatorilor, a locului de unde are loc accesul şi a datelor accesate, inclusiv a celor cu caracter personal;

e) utilizarea sistemelor de autentificare care folosesc cel puţin doi factori;

f) să se asigure că utilizatorii autorizaţi nu furnizează elementele de autentificare către terţe persoane.

Art. 17. - (1) Entităţile au obligaţia să testeze anual planul de răspuns la incidente de securitate informatică.

(2) Planul de răspuns la incidente de securitate informatică trebuie să prevadă simularea unui incident de securitate informatică şi să acopere toate sistemele informatice şi reţelele utilizate de către entitate.

Art. 18. - (1) Entităţile au obligaţia ca, în termen de maximum 45 de zile de la finalizarea testării prevăzute la art. 17, să întocmească un raport de testare care va cuprinde următoarele informaţii, fără a se limita la acestea:

a) modalitatea de aplicare a fiecărei etape din planul de răspuns la incidente de securitate informatică;

b) modalitatea de gestionare a comunicării interne şi externe pe toată durata testării;

c) cauzele şi impactul real/potenţial al incidentului de securitate informatică asupra datelor entităţii;

d) propuneri pentru îmbunătăţirea măsurilor de securitate la incidente informatice;

e) propuneri pentru îmbunătăţirea planului de răspuns la incidente de securitate informatică.

(2) Raportul de testare prevăzut la alin. (1) este păstrat la sediul entităţii care are obligaţia să îl prezinte auditorului IT şi A.S.F. la solicitarea acesteia.

Art. 19. - Sistemele informatice importante care oferă intermediarilor şi clienţilor acestora accesul la platforme electronice de tranzacţionare, precum şi sistemele informatice importante care evidenţiază operaţiuni de compensare, decontare şi registru pentru instrumente financiare şi operaţiuni cu aceste instrumente, asigură, fără a se limita la acestea:

a) securitatea şi integritatea datelor procesate prin folosirea unei modalităţi de securizare atât asupra datelor trimise către platformele electronice de tranzacţionare şi către cele de compensare, decontare şi registru, cât şi asupra datelor recepţionate de la aceste platforme;

b) mecanisme care să garanteze nerepudierea datelor transmise şi recepţionate;

c) jurnalizarea în timp real a informaţiei despre ordinele transmise spre executare, a stării acestor ordine, respectiv a modificărilor care se aduc acestor ordine în decursul existenţei lor de către clienţii şi intermediarii care utilizează aceste sisteme informatice importante;

d) mecanisme de nerepudiere a integrităţii înregistrării operaţiunilor de sistem informatic important.

Art. 20. - Sistemele informatice care oferă S.A.I./A.F.I.A. şi investitorilor acestora accesul la platforme electronice de distribuire a titlurilor de participare asigură, fără a se limita la acestea:

a) securitatea şi integritatea datelor procesate prin folosirea unei modalităţi de securizare asupra datelor trimise către platformele electronice de distribuire a titlurilor de participare;

b) mecanisme care să garanteze nerepudierea datelor transmise şi recepţionate;

c) jurnalizarea în timp real a informaţiei despre instrucţiunile investitorilor transmise către S.A.I./A.F.I.A.;

d) mecanisme de nerepudiere a integrităţii înregistrării operaţiunilor de sistem informatic.

CAPITOLUL IV
Auditarea şi testarea sistemelor informatice importante

SECŢIUNEA 1
Dispoziţii privind auditul IT

Art. 21. - (1) Entităţile au obligaţia de a audita sistemele informatice importante, după cum urmează:

a) entităţile încadrate în categoria de risc major au obligaţia de a audita IT extern sistemele informatice importante utilizate, cu periodicitate anuală, astfel încât perioada supusă auditului să fie un an calendaristic, începând cu prima lună ianuarie după data sfârşitului perioadei supuse auditului IT anterior;

b) entităţile încadrate în categoria de risc important au obligaţia de a audita IT extern sau cu resurse interne certificate sistemele informatice importante utilizate, o dată la 2 ani, astfel încât

perioada supusă auditului să fie 2 ani calendaristici consecutivi, începând cu prima lună ianuarie după data sfârşitului perioadei supuse auditului IT anterior;

c) entităţile încadrate în categoria de risc mediu au obligaţia de a audita IT extern sau cu resurse interne certificate sistemele informatice importante utilizate, o dată la 3 ani, astfel încât perioada supusă auditului să fie 3 ani calendaristici consecutivi, începând cu prima lună ianuarie după data sfârşitului perioadei supuse auditului IT anterior;

d) entităţile încadrate în categoria de risc scăzut au obligaţia de a audita IT extern sau cu resurse interne certificate sistemele informatice importante utilizate, o dată la 4 ani, astfel încât perioada supusă auditului să fie 4 ani calendaristici consecutivi, începând cu prima lună ianuarie după data sfârşitului perioadei supuse auditului IT anterior.

(2) Perioada supusă auditului IT reprezintă perioada cuprinsă între două audituri succesive.

Art. 22. - Entităţile care efectuează auditul IT cu resurse interne certificate au obligaţia să utilizeze personal certificat în domeniul auditării IT, angajat în cadrul entităţii sau în cadrul unei companii din cadrul aceluiaşi grup financiar, cu respectarea prevederilor prezentei norme şi a metodologiilor certificate internaţional.

Art. 23. - (1) Auditul IT extern se efectuează în baza unui contract de audit IT încheiat între entitatea care a solicitat auditarea şi un auditor IT extern înscris în Lista auditorilor IT externi menţinută de A.S.F. în conformitate cu prevederile art. 38.

(2) Entitatea nu poate contracta auditul IT cu acelaşi auditor IT extern pentru mai mult de 3 audituri consecutive efectuate în conformitate cu prevederile art. 21.

Art. 24. - Entitatea are obligaţia de a se asigura că în contractul de audit IT sunt cuprinse în mod obligatoriu clauze cu privire la faptul că auditorul IT extern trebuie să respecte cerinţele impuse pentru efectuarea auditului sistemelor informatice importante, în conformitate cu prevederile prezentei norme şi cu bunele practici în domeniu.

Art. 25. - Auditorul IT extern notifică în scris A.S.F. în cel mai scurt timp posibil, dar nu mai târziu de 10 zile de la constatare, orice fapt sau act în legătură cu sistemele informatice importante utilizate de către aceasta şi care:

a) este de natură să afecteze continuitatea activităţii entităţii auditate;

b) poate conduce la o opinie de audit cu rezerve, la imposibilitatea exprimării unei opinii de audit sau la o opinie de audit negativă.

Art. 26. - La solicitarea scrisă a A.S.F., auditorul IT extern comunică A.S.F., în termen de maximum 10 zile de la solicitare, următoarele:

a) orice raport sau document care a fost adus la cunoştinţa entităţii auditate;

b) o declaraţie care să indice motivele de încetare a contractului de audit IT, indiferent de natura acestora;

c) orice alte informaţii sau documente solicitate în legătură cu activitatea de audit IT extern.

Art. 27. - Auditorul IT care efectuează activitatea de audit IT la entităţile prevăzute la art. 2 are obligaţia de a întocmi şi de a prezenta conducerii entităţii o situaţie a deficienţelor şi vulnerabilităţilor identificate.

Art. 28. - La finalizarea auditului IT, auditorii IT au obligaţia de a întocmi un raport de audit IT însoţit de anexe, care să cuprindă cel puţin elementele prevăzute în macheta de raportare prezentată în anexa nr. 3, dar fără a se limita la acestea.

Art. 29. - (1) A.S.F. poate să instituie în sarcina entităţii obligaţia de a audita IT orice sisteme informatice dacă:

a) în urma constatărilor rezultă că entitatea nu a desfăşurat toate activităţile minime obligatorii categoriei de risc în care aceasta a fost încadrată, conform prevederilor art. 10 sau 11, sau activităţile desfăşurate au un caracter formal;

b) apreciază că se impune efectuarea unor investigaţii suplimentare la nivelul sistemelor informatice.

(2) Instituirea de către A.S.F. a obligaţiei de a audita IT alte sisteme informatice conform alin. (1) cuprinde şi termenul până la care entitatea este obligată să transmită la A.S.F. raportul de audit, iar acest termen nu poate să depăşească 90 de zile de la data instituirii obligaţiei de a audita alte sisteme informatice de către A.S.F.

Art. 30. - Entităţile, inclusiv cele care efectuează auditul IT cu resurse interne certificate, sunt obligate să adopte toate măsurile necesare pentru evitarea conflictelor de interese care pot interveni în desfăşurarea activităţii de audit IT.

Art. 31. - Entităţile, inclusiv cele care efectuează auditul IT cu resurse interne certificate, sunt obligate să se asigure că activitatea de audit IT este independentă faţă de activitatea auditată, pentru a nu fi compromisă obiectivitatea acesteia, iar auditorii IT sunt independenţi şi obiectivi în toate aspectele legate de activitatea de audit IT.

Art. 32. - În aplicarea prevederilor art. 31, entităţile care efectuează auditul IT cu resurse interne certificate sunt obligate:

a) să se asigure că auditorul IT notifică în scris A.S.F. în cel mai scurt timp posibil, dar nu mai târziu de 10 zile de la constatare, orice fapt sau act în legătură cu sistemele informatice importante utilizate de către aceasta şi care este de natură să afecteze continuitatea activităţii entităţii auditate sau poate conduce la o opinie de audit cu rezerve, la imposibilitatea exprimării unei opinii de audit sau la o opinie de audit negativă;

b) să prezinte, la solicitarea A.S.F., în termen de maximum 10 zile, orice raport sau document care a fost adus la cunoştinţa entităţii auditate sau orice alte informaţii ori documente solicitate în legătură cu activitatea de audit IT.

Art. 33. - Entităţile, inclusiv cele care efectuează auditul IT cu resurse interne certificate, sunt obligate să furnizeze auditorului IT informaţii complete, corespunzătoare, relevante şi în timp util, pentru a permite desfăşurarea în bune condiţii a activităţii de audit IT.

Art. 34. - Respectarea prevederilor art. 25 şi 26 nu contravine conduitei etice şi profesionale, nu constituie o încălcare a secretului profesional impus prin clauze contractuale sau prin prevederi legale şi nu atrage niciun fel de răspundere asupra persoanei fizice şi/sau juridice în cauză.

SECŢIUNEA a 2-a
Testarea sistemelor informatice importante

Art. 35. - (1) Entitatea are obligaţia de a ţine evidenţa următoarelor modificări majore ale sistemelor informatice importante:

a) schimbarea integrală a sistemelor/programelor informatice importante;

b) externalizarea unor servicii IT;

c) schimbarea proceselor de arhivare electronică, de restaurare sau sincronizare a bazelor de date.

(2) În situaţia dezafectării unui sistem informatic important, entitatea are obligaţia să solicite efectuarea unui audit IT cu resurse interne certificate sau externe care vizează sistemele ce urmează a fi dezafectate.

Art. 36. - (1) Entitatea are obligaţia să testeze sistemele informatice importante înainte de prima utilizare şi la orice modificare în cadrul ciclului de viaţă al acestora, indiferent dacă sunt realizate cu resurse interne sau de către furnizori externi.

(2) Rezultatul testărilor prevăzute la alin. (1) se consemnează într-un raport de testare IT care cuprinde, fără a se limita la acestea, următoarele elemente:

a) echipa de testare;

b) scopul testării;

c) perioada testării;

d) descrierea programului informatic testat;

e) identificarea aplicaţiilor utilizate şi a persoanelor implicate;

f) analiza riscurilor implicate de achiziţia sau modificarea programului informatic, a posibilelor vulnerabilităţi şi a măsurilor de reducere a riscurilor asociate, prin controale de sistem sau de program informatic;

g) descrierea modului în care s-au efectuat testele, scenariile de test, eventualele norme sau standarde aplicate şi rezultatul testării;

h) concluzia echipei de testare;

i) semnătura membrilor echipei de testare.

Art. 37. - Entitatea are obligaţia să păstreze rapoartele de testare IT pentru o perioadă de cel puţin 5 ani după momentul dezafectării sistemului informatic important şi să le pună la dispoziţia A.S.F. sau auditorului IT, la cerere.

CAPITOLUL V
Înscrierea auditorul IT extern

Art. 38. - Auditorul IT extern care intenţionează să presteze servicii de audit IT pentru entităţile cărora le sunt incidente prevederile prezentei norme are obligaţia înscrierii în Lista auditorilor IT externi menţinută de A.S.F.

Art. 39. - În vederea înscrierii în lista prevăzută la art. 38, auditorul IT extern depune la A.S.F. o cerere, în care menţionează sectorul/sectoarele în care activează entităţile pentru care intenţionează să presteze servicii de audit IT, însoţită de documentaţia care trebuie să cuprindă următoarele, după caz:

a) datele de identificare ale auditorului IT extern:

1. numele complet/denumirea şi adresa/sediul - adresa completă;

2. adresa unde îşi desfăşoară activitatea;

3. telefon/fax, e-mail, adresa paginii de internet;

b) pentru auditorul IT persoană fizică certificată şi reprezentantul societăţii de audit IT extern, care vor semna raportul de audit, se depun următoarele documente, după caz:

1. actul de identitate al auditorului IT, în copie;

2. curriculum vitae al auditorului IT, datat şi semnat, cu prezentarea experienţei profesionale în auditarea IT externă a sistemelor informatice;

3. certificatul de auditor IT, în copie, semnată pentru conformitate cu originalul, din care reiese experienţa în domeniul de audit IT extern al sistemelor informatice;

4. dovada experienţei şi a specializării pe domeniul de audit IT extern al sistemelor informatice;

5. certificat constatator emis de Oficiul Naţional al Registrului Comerţului, cu starea la zi a persoanei juridice, în original;

6. certificatul de cazier judiciar şi certificatul de cazier fiscal, în original, aflate în termenul de valabilitate;

7. contractul de asigurare de răspundere civilă profesională a auditorului IT extern, pentru suma asigurată de minimum 100.000 euro, valabil la data depunerii documentaţiei, în copie;

8. documentul de plată a tarifului de înscriere în Registrul public al A.S.F., în copie.

Art. 40. - Înscrierea auditorului IT extern în Lista auditorilor IT externi sau transmiterea refuzului motivat al înscrierii se efectuează de A.S.F. în termen de maximum 30 de zile de la primirea dosarului complet al solicitantului.

Art. 41. - Orice modificare a documentaţiei prevăzute la art. 39 lit. b) pct. 1, 3, 5, 6 şi 7 trebuie transmisă A.S.F. în termen de maximum 30 de zile de la data efectuării modificării.

Art. 42. - A.S.F. radiază din lista prevăzută la art. 38 auditorii IT externi în oricare dintre următoarele situaţii:

a) la cererea acestora;

b) în cazul lichidării sau la declanşarea insolvenţei;

c) în cazul încălcării prevederilor art. 25, 26, 28 şi 41;

d) în cazul nerespectării prevederilor prezentei norme.

Art. 43. - Pentru toate situaţiile menţionate la art. 42 lit. c) şi d), A.S.F. transmite auditorului IT extern o notificare prealabilă prin care i se aduc la cunoştinţă faptele pentru care A.S.F. va proceda la iniţierea demersurilor pentru radierea din Lista auditorilor IT externi.

CAPITOLUL VI

Dispoziţii privind furnizorii externi şi furnizorii de servicii IT externalizate pentru sistemele informatice importante

Art. 44. - Orice externalizare de servicii se realizează cu respectarea legislaţiei aplicabile entităţii.

Art. 45. - În situaţiile în care entităţii nu îi sunt aplicabile alte prevederi legale referitoare la externalizarea unor servicii IT şi în toate cazurile în care sunt utilizate serviciile unor furnizori externi, pentru toate sistemele informatice importante, entitatea are obligaţia de a notifica la A.S.F. furnizorul extern sau furnizorul de servicii IT externalizate, în termen de maximum 14 zile de la data încheierii contractului cu acesta.

Art. 46. - **(1)** Notificarea prevăzută la art. 45 trebuie să conţină următoarele informaţii şi documente, după caz:

a) descrierea serviciilor furnizate/externalizate;

b) datele de identificare a furnizorului:

1. sediul societăţii - adresa completă;

2. telefon/fax, e-mail, pagina de internet;

c) certificat constatator emis de Oficiul Naţional al Registrului Comerţului, cu starea la zi a persoanei juridice, sau echivalentul acestuia pentru furnizorii externi înregistraţi în alte state, în original sau copii conforme cu originalul;

d) documente în funcţie de tipul serviciului sau activităţii desfăşurate, astfel:

1. SR ISO/IEC 27001 sau certificări pentru standarde echivalente - pentru toţi furnizorii;

2. certificări pentru furnizarea şi dezvoltarea de programe informatice software;

3. certificări pentru furnizarea de servicii externalizate;

4. act doveditor privind respectarea condiţiilor tehnice conform TIA-942 nivel 2 sau echivalent pentru furnizarea de servicii de găzduire sau externalizare prin intermediul centrelor de date;

5. autorizare pentru furnizarea de servicii de arhivare electronică prin centre de date;

6. certificate specifice activităţilor externalizate pentru furnizarea de servicii externalizate de tip cloudcomputing public.

(2) Certificările prevăzute la alin. (1) lit. d) pct. 1, 2, 3 şi 6 trebuie să fie emise de entităţi/organisme abilitate/recunoscute pe plan intern şi/sau internaţional.

Art. 47. - Entitatea are obligaţia ca, în cazul modificării unor informaţii şi/sau documente prevăzute la art. 46, care pot conduce la afectarea desfăşurării serviciilor externalizate conform contractului, să notifice A.S.F. şi să depună originalul sau copia documentelor modificate în termen de maximum 90 de zile de la data efectuării modificării.

Art. 48. - Pentru sistemele informatice importante, entitatea are obligaţia să se asigure că furnizorii de servicii IT externalizate, inclusiv în cazul externalizărilor în lanţ, cu excepţia furnizorilor de servicii de comunicaţii, de hardware sau de licenţe software, raportat strict la activitatea externalizată:

a) permit respectarea de către entitate a prevederilor prezentei norme, astfel încât prin externalizarea anumitor activităţi să nu se încalce legislaţia aplicabilă;

b) prezintă, la solicitarea A.S.F., modalitatea prin care sunt îndeplinite de către entitate prevederile prezentei norme;

c) permit A.S.F. şi auditorului IT să verifice şi/sau să auditeze sistemele sale informatice în contextul aplicării prevederilor prezentei norme sau pun la dispoziţia auditorului IT un raport de audit IT întocmit în conformitate cu standardele ISAE 3402 sau echivalent pentru sistemele informatice puse la dispoziţia entităţii.

CAPITOLUL VII
Dispoziţii privind raportarea

Art. 49. - Entitatea are obligaţia să întocmească în conformitate cu prevederile prezentei norme şi ale altor reglementări incidente şi să transmită A.S.F. următoarele rapoarte:

a) raportul anual privind evaluarea internă a riscurilor operaţionale efectuată în conformitate cu prevederile art. 6 alin. (1), până la data de 31 martie a anului curent;

b) raportul de audit IT întocmit pentru perioada supusă auditului pentru auditul IT efectuat în conformitate cu art. 21, până la data de 30 iunie a anului curent, după ultimul an din perioada supusă auditului, însoţit de copia certificatului de auditor IT semnată pentru conformitate cu originalul valabil la momentul întocmirii raportului de audit;

**) Potrivit art. 2 alin. (2) din Norma Autorităţii de Supraveghere Financiară nr. 21/2020, termenul prevăzut la art. 49 lit. b) din Norma Autorităţii de Supraveghere Financiară nr. 4/2018 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară, cu modificările ulterioare, privind depunerea raportului de audit IT realizat în anul 2020 se prorogă până la data de 31 decembrie 2020.*

c) raportarea electronică anuală cu indicatorii menţionaţi în anexa nr. 4, în cazul în care aceşti indicatori sunt aplicabili şi sunt aferenţi sistemelor informatice importante, până la data de 31 martie a anului curent, pentru anul anterior.

Art. 50. - În cazul în care au fost identificate deficienţe/vulnerabilităţi în conformitate cu prevederile art. 27, raportul de audit IT prevăzut la art. 49 lit. b) se transmite A.S.F. însoţit de planul de acţiune din care să rezulte modalitatea de remediere a deficienţelor/vulnerabilităţilor identificate de auditorul IT.

Art. 51. - Rapoartele prevăzute la art. 49 se transmit A.S.F., în conformitate cu sistemul de raportare comunicat acestora de fiecare structură organizatorică din cadrul A.S.F. cu atribuţii de supraveghere, pe suport hârtie sau în format electronic cu semnătură electronică extinsă, după caz.

CAPITOLUL VIII
Dispoziţii tranzitorii şi finale

Art. 52. - Nerespectarea prevederilor prezentei norme de către entităţile prevăzute la art. 2 constituie contravenţie conform prevederilor Legii nr. 236/2018 privind distribuţia de asigurări, cu completările ulterioare, ale Legii nr. 237/2015 privind autorizarea şi supravegherea activităţi de asigurare şi reasigurare, cu modificările şi completările ulterioare, ale Legii nr. 297/2004 privind piaţa de capital, cu modificările şi completările ulterioare, ale Ordonanţei de urgenţă a Guvernului nr. 32/2012 privind organismele de plasament colectiv în valori mobiliare şi societăţile de administrare a investiţiilor, precum şi pentru modificarea şi completarea Legii nr. 297/2004 privind piaţa de capital, aprobată cu modificări şi completări prin Legea nr. 10/2015, cu modificările şi completările ulterioare, ale Legii nr. 74/2015 privind administratorii de fonduri de investiţii alternative, cu modificările şi completările ulterioare, ale Legii nr. 126/2018 privind pieţele de instrumente financiare, ale Legii nr. 411/2004 privind fondurile de pensii administrate privat, republicată, cu modificările şi completările ulterioare, ale Legii nr. 204/2006 privind pensiile facultative, cu modificările şi completările ulterioare, ale Legii nr. 1/2020 privind pensiile ocupaţionale, ale Legii nr. 187/2011 privind înfiinţarea, organizarea şi funcţionarea Fondului de garantare a drepturilor din sistemul de pensii private, ale Legii nr. 213/2015 privind Fondul de garantare a asiguraţilor şi ale Legii nr. 132/2017 privind asigurarea obligatorie de răspundere civilă auto pentru prejudicii produse terţilor prin accidente de vehicule şi tramvaie.

Art. 53. - **(1)** Începând cu anul 2018, entităţile au obligaţia să respecte termenele de raportare prevăzute la art. 49.

(2) Biroul asigurătorilor de autovehicule din România efectuează primele raportări pentru anul 2018 începând cu anul 2019, în termenele prevăzute la art. 49.

Art. 54. - **(1)** Prevederile prezentei norme se aplică entităţilor care nu au în derulare auditul IT la data publicării prezentei norme în Monitorul Oficial al României, Partea I.

(2) Auditul IT în curs de desfăşurare la data intrării în vigoare a prezentei norme va continua în conformitate cu reglementările în vigoare la data începerii auditului IT.

Art. 55. - Anexele nr. 1-4 fac parte integrantă din prezenta normă.

Art. 56. - Prezenta normă se publică în Monitorul Oficial al României, Partea I, şi intră în vigoare în termen de 30 de zile de la data publicării.

Art. 57. - La data intrării în vigoare a prezentei norme se abrogă Norma Autorităţii de Supraveghere Financiară nr. 6/2015 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de Autoritatea de Supraveghere Financiară, publicată în Monitorul Oficial al României, Partea I, nr. 227 din 3 aprilie 2015, cu modificările şi completările ulterioare.

Preşedintele Autorităţii de Supraveghere
Financiară,
Leonardo Badea

Bucureşti, 28 februarie 2018.
Nr. 4.

ANEXA Nr. 1

Definiţii şi abrevieri

1. arhivare electronică - stocarea documentelor în format digital;

2. analiză de risc - analiza scenariilor de ameninţări semnificative, pentru a evalua probabilitatea materializării acestora şi impactul potenţial pe care un astfel de eveniment l-ar avea asupra entităţii şi operaţiunilor acesteia;

3. atac etic/test de penetrare - test al sistemelor informatice realizat printr-o simulare a unui atac real asupra reţelelor, sistemelor şi programelor informatice utilizate de entitatea testată sau auditată, după caz;

4. audit IT -activitatea de colectare şi evaluare a unor probe pentru a determina dacă sistemul informatic respectă parametrii de performanţe şi de lucru conform cerinţelor de proiectare, dacă asigură funcţionalităţile necesare cerinţelor de afaceri şi respectarea legislaţiei în domeniu, dacă este securizat, dacă menţine integritatea datelor prelucrate şi stocate, dacă permite atingerea obiectivelor strategice ale entităţii şi utilizarea eficientă a resurselor informaţionale;

5. auditor IT - persoana fizică autorizată care deţine certificat de auditor IT sau persoană juridică cu personal certificat, care derulează o activitate de auditare a sistemelor informatice, conform reglementărilor şi bunelor practici în domeniu;

6. bază de date - structură de organizare a informaţiei în unul sau mai multe domenii de aplicare, cu scopul de a o face accesibilă în permanenţă către utilizatori prin ansamblul de programe informatice;

7. centru de date - spaţiu securizat, dotat cu tehnică de calcul şi echipamente de comunicaţii prin intermediul cărora se primesc, se stochează şi se transmit date în formă electronică, care se implementează respectând standardele specifice, utilizând conceptul de nivel sau un echivalent al acestuia, precum, dar fără a se limita la, standardele SR EN 50600 (European Standard - Data Centers Facilities and Infrastructures) sau TIA-942 (Telecommunications Industry Association);

8. centru de date de nivel 2 - centru de date care îndeplineşte cerinţele TIA-942 tier 2 sau echivalent şi a cărui infrastructură prezintă caracteristicile de disponibilitate de 99,741%, circuit dedicat pentru răcire şi alimentare cu energie electrică, include componente redundante, include podea înălţată, surse neîntreruptibile de putere, generator şi se încadrează într-un număr de maximum 22 de ore de nefuncţionare pe an;

9. ciclu de viaţă - totalitatea stadiilor din viaţa unui serviciu IT, a unui element de configuraţie, a unui incident, a unei probleme sau a unei schimbări, fără a se limita la acestea;

10. cloud computing public - infrastructură informatică, cu resurse de calcul configurabile, care permite furnizarea la cerere de servicii IT şi este asigurată prin centre de date publice, altele decât infrastructura informatică proprie entităţii, prin intermediul unui furnizor extern,

ca un ansamblu distribuit de servicii de calcul, programe informatice, acces la informaţii şi stocare de date;

11. comunicaţii/telecomunicaţii - sisteme de transmisie, precum şi orice alte resurse care permit transportul semnalelor prin fir, radio, fibră optică sau orice alte mijloace electromagnetice, precum şi tehnologiile utilizate în cadrul proceselor de comunicare, care presupun existenţa unui mediu informatic constituit din echipamente hardware, software specializat, precum şi dispozitive electronice de transmisie/recepţie date;

12. controale informatice - totalitatea politicilor, procedurilor, practicilor şi a structurilor organizaţionale informatice proiectate să ofere o asigurare rezonabilă asupra faptului că obiectivele afacerii vor fi atinse şi evenimentele nedorite vor fi prevenite sau detectate şi corectate;

13. date (informatice) - orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, incluzându-se şi orice program informatic care poate determina realizarea unei funcţii similare de către un sistem informatic;

14. disponibilitate - capabilitatea unui serviciu IT sau unui element de configuraţie IT de a efectua funcţiile agreate atunci când este necesar acest lucru;

15. dubla validare/validare dublă - validarea unei acţiuni de către doi utilizatori sau existenţa unei validări informatice duble ce implică un program care verifică o anumită acţiune prin metode diferite;

16. externalizare servicii IT - utilizarea de către o entitate a unui furnizor extern de servicii IT, în vederea desfăşurării de către acesta, pe bază contractuală şi în mod continuu sau pentru o perioadă, a operaţiunilor aferente suportului tehnic sau al procesării, necesare desfăşurării activităţii efectuate în mod obişnuit de către entitatea în cauză;

17. externalizare în lanţ - externalizare în cadrul căreia furnizorul extern subcontractează cu alţi furnizori externi elemente componente ale serviciilor prestate entităţii;

18. furnizor extern - persoană juridică sau fizică autorizată furnizoare de bunuri (precum hardware, licenţe software, componente etc.) şi soluţii informatice, care deţine expertiză în domenii specializate, cu respectarea cadrului legal aplicabil;

19. furnizor de servicii IT externalizate - persoană juridică sau persoană fizică autorizată cu obiect de activitate şi expertiză în domeniul serviciilor informatice, furnizoare de servicii informatice în condiţiile respectării cadrului legal aplicabil şi a autorizării primite;

20. hardware - ansamblul elementelor fizice şi tehnice cu ajutorul cărora datele se pot culege, verifica, prelucra, transmite, afişa şi stoca, inclusiv suporturile de memorare a datelor, precum şi echipamentele de calculator auxiliare;

21. incident de securitate - eveniment înregistrat şi declarat la nivelul entităţii privind securitatea informaţiei sau a sistemelor informatice cu o probabilitate semnificativă de compromitere a operaţiunilor şi de ameninţare a securităţii IT a cărei consecinţă a determinat sau este de natură să determine compromiterea informaţiilor sau a sistemelor informatice;

22. indicatori-cheie de performanţă (KPI) - parametri analitici reprezentativi selectaţi pentru monitorizarea unor activităţi şi procese-cheie pentru entităţi, oferind o privire de ansamblu asupra performanţei;

23. indicatori-cheie de risc (KRI) - parametrii care măsoară efectiv riscurile aferente procedurilor şi activităţilor entităţii, furnizând în timp semnalări corespunzătoare ale consecinţelor cu efect negativ, care pot genera potenţiale pierderi directe sau indirecte;

24. indisponibilitate (ca durată în timp) - intervalul de timp din cadrul perioadei agreate ca disponibilitate a serviciului, în care un serviciu IT sau o componentă critică/importantă a serviciului nu este disponibilă;

25. informaţie - rezultatul prelucrării datelor printr-un sistem informatic care sunt baza pentru asigurarea cunoaşterii prin intermediul unor elemente noi în raport cu cunoştinţele anterioare şi constituie o resursă care trebuie protejată;

26. infrastructura informatică - elemente ale bazei tehnico- materiale, pe componente sau ca sistem, care susţin culegerea, stocarea şi managementul datelor, precum şi integrarea, căutarea şi vizualizarea datelor şi alte calcule şi servicii de procesare a informaţiei utilizând tehnologii informatice, deţinute sau contractate extern de către entitate şi necesare bunei funcţionări a acesteia;

27. integritate - păstrarea datelor electronice, digitalizate, nealterate pe timpul comunicaţiei dintre corespondenţi sau pe perioada de stocare a datelor;

28. ISACA - Asociaţia de Audit şi Control al Sistemelor Informatice/Information Systems Audit and Control Association;

29. ISAE 3402 - standard de audit utilizat pentru obţinerea unor rapoarte de asigurare privind controalele din cadrul unei organizaţii prestatoare de servicii;

30. SR ISO/IEC 27001 - standard care stabileşte cerinţele pentru un sistem de management al securităţii informaţiei;

31. managementul schimbării - procesul responsabil cu controlul ciclului de viaţă al tuturor schimbărilor pentru a permite implementarea schimbărilor benefice cu minimum de întrerupere a serviciilor IT;

32. nerepudiere - atribut care să prevină posibilitatea unei entităţi de a nega o acţiune întreprinsă în context informaţional;

33. plan de cooperare în domeniul securităţii reţelelor şi a informaţiei - plan care stabileşte rolurile organizaţionale, obligaţiile şi răspunderile în cadrul cooperării, precum şi procedurile de menţinere sau de restabilire a funcţionării reţelelor şi sistemelor informatice în cazul în care acestea sunt afectate de un risc sau de un incident cibernetic cu impact semnificativ;

34. program informatic (aplicaţie) - ansamblu de instrucţiuni care poate fi executat de un sistem informatic în vederea obţinerii unui rezultat determinat;

35. resurse informaţionale - totalitatea informaţiilor şi a documentelor, conform cerinţelor stabilite de legislaţia în domeniu; utilizat doar în definiţia auditului IT;

36. reţea - ansamblu de echipamente legate între ele prin canale de transmisie, precum, dar fără a se limita la, o reţea de calculatoare;

37. risc de securitate - orice circumstanţă sau eveniment care are un efect negativ potenţial asupra securităţii sistemelor informatice;

38. risc sistemic - riscul de afectare a unei zone importante a sistemului financiar sau a unei pieţe financiare, cu potenţial de consecinţe negative serioase pentru piaţa internă şi economia reală, instabilitate a sistemului financiar, posibil catastrofică, cauzată sau accentuată de evenimente idiosincratice sau de condiţii ale entităţilor;

39. riscuri semnificative - riscuri cu impact însemnat asupra situaţiei financiare, patrimoniale şi/sau reputaţionale a entităţilor;

40. raport de audit IT - instrumentul prin care se comunică scopul auditării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările şi concluziile auditului, precum şi orice rezervă pe care auditorul IT o are asupra sistemului informatic auditat;

41. raport de testare IT - instrumentul prin care se comunică scopul testării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările şi concluziile testării, precum şi orice rezervă pe care echipa de testare o are asupra sistemului informatic testat;

42. risc aferent tehnologiei informaţiei (IT) - subcomponentă a riscului operaţional care se referă la riscul actual sau viitor de afectare negativă, pe de o parte, a profiturilor şi capitalului entităţilor sau a investitorilor, participanţilor sau asiguraţilor, pe de altă parte, determinat de inadecvarea strategiei şi politicilor IT, a tehnologiei informaţiei şi a procesării acesteia, din punctul de vedere al capacităţii de gestionare, integritate, controlabilitate şi continuitate, sau de utilizare necorespunzătoare a tehnologiei informaţiei;

43. securitate (cibernetică) - capacitatea unei reţele sau a unui sistem informatic, rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive, de a rezista, la un nivel de încredere dat, unei acţiuni accidentale sau răuvoitoare care compromite disponibilitatea, autenticitatea, integritatea sau confidenţialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de reţeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;

44. semnătură electronică (digitală) - atribut indispensabil al documentului electronic, obţinut în urma transformării criptografice a acestuia, cu utilizarea cheii private, conform prevederilor Legii nr. 455/2001 privind semnătura electronică, republicată;

45. serviciu IT - combinaţie de persoane, procese şi tehnologii furnizate în interiorul entităţii sau de către un furnizor de servicii IT, care se bazează pe folosirea tehnologiei informaţiei şi care asigură suportul tehnic necesar desfăşurării activităţii entităţii şi care ar trebui să fie definită într-un acord al nivelului agreat de serviciu (SLA);

46. sistem informatic - ansamblu de elemente intercorelate funcţional în scopul automatizării obţinerii informaţiilor necesare activităţilor operaţionale şi manageriale într-o entitate, prin intermediul serviciilor IT, al echipamentelor hardware şi produselor software, proceduri manuale, baze de date şi modele matematice pentru analiză, planificare, control şi luarea deciziilor, utilizând componente de introducere şi prelucrare date, componente de procesare precum servere, calculatoare, sisteme software de operare de bază, programe informatice, reţele de calculatoare şi telecomunicaţii, componente de stocare şi utilizatori, fără ca enumerarea să fie limitativă;

47. software - toată gama de produse program, care cuprinde cel puţin următoarele elemente: sisteme de operare, drivere sau programe informatice;

48. tehnologia informaţiei (IT) sau tehnologia informaţiei şi a comunicaţiilor - tehnologia necesară pentru prelucrarea (procurarea, procesarea, stocarea, convertirea şi transmiterea) informaţiei, în particular prin folosirea calculatoarelor electronice şi a programelor corespunzătoare;

49. TIA-942 - standard ce defineşte infrastructura unui centru de date, în mod special din privinţa sistemului de cablare şi a designului reţelei, dar acoperă şi locaţia, răcirea, alimentarea cu energie electrică şi amenajarea sa, precum şi considerente legate de mediu;

50. vulnerabilităţi - stări de fapt, procese şi/sau fenomene care diminuează capacitatea de reacţie a sistemelor informatice la riscurile existente ori potenţiale sau care favorizează apariţia şi dezvoltarea lor, cu consecinţe în planul funcţionalităţii şi utilităţii.

ANEXA Nr. 2

Activităţi obligatorii desfăşurate de către entităţi

Entităţile vor desfăşura activităţile precizate în tabelul de mai jos, conform categoriilor de risc corespunzătoare.

Activităţi obligatorii ale entităţilor, pe categorii de risc

	Activitate	Categoria de risc a entităţii			
		Majoră	Importantă	Medie	Scăzută
A. Evaluare internă a riscului operaţional şi registrul riscurilor		x	x	x	x
B. Organizare pe procese					
1	Management disponibilitate	x	x	x	
2	Management utilizatori	x	x	x	x
3	Management incidente	x	x	x	
4 Management schimbare					
a)	Management ciclu viaţă programe informatice	x	x	x	x
b)	Management versiuni	x	x	x	x
c)	Management testare	x	x	x	x
5	Management capacitate	x	x	x	
6	Management configuraţii	x	x		
7	Management niveluri servicii (SLA)	x	x	x	
8 Management securitate					
a)	Cerinţe generale	x	x	x	x
b)	Scanare de vulnerabilităţi	x	x	x	x
c)	Teste de penetrare[1]	x	x	x	
9	Management continuitate	x	x	x	
C. Puncte de control şi măsură					
1	Controale generale	x	x	x	
2	Controale program informatic	x	x		
3	Controale flux financiar	x	x	x	x
D. Implementare indicatori-cheie de performanţă (KPI)		x			
E. Implementare indicatori-cheie de risc (KRI)		x	x		

F. Managementul securităţii sistemului informatic					
1	Măsuri organizatorice	x	x		
2	Proceduri de securitate	x	x	x	x
3	Evaluare securitate	x			
4	Plan de cooperare	x	x	x	x

[1] Pentru raportare testul de penetrare va fi efectuat în perioada auditată.

ANEXA Nr. 3

Machetă de raportare

I. Raportul de audit IT
II. Anexe la raportul de audit IT:
1. Sumarul observaţiilor
2. Analiza internă a riscurilor operaţionale şi registrul riscurilor
3. Cerinţe referitoare la furnizorii externi şi furnizorii de servicii IT externalizate pentru sistemele informatice importante
4. Organizarea pe procese
5. Concluzii ale echipei de audit privind respectarea cerinţelor impuse
6. Declaraţia pe propria răspundere a auditorului IT extern
7. Declaraţie pe propria răspundere a reprezentantului legal al entităţii auditate IT cu resurse interne

I. Raportul de audit IT

#	Capitol	Comentarii/Explicaţii
A	Titlul raportului	
B	Destinatarii raportului şi orice restricţii privind conţinutul şi circulaţia raportului	
C	Paragraf introductiv	Identificarea entităţii auditate (Denumire/Numărul de înregistrare la Oficiul Naţional al Registrului Comerţului/Adresă) Includerea afirmaţiei că sistemele informatice au fost auditate ca urmare a obligaţiei legale impuse de prezenta normă
D	Asumarea responsabilităţii conducerii entităţii privind auditul efectuat asupra sistemelor informatice	

<table>
<tr><td>E</td><td>Responsabilitatea auditorului IT</td><td>Raportul de audit IT va include cel puţin afirmaţiile:
- că "este responsabilitatea auditorului IT să exprime o opinie cu privire la conformitatea sistemelor informatice cu prevederile prezentei norme";
- că raportul de audit IT a fost elaborat în conformitate cu standardul de audit utilizat, respectiv. . . (menţionarea acestuia)</td></tr>
<tr><td>F</td><td>Datele de identificare ale coordonatorului certificat al echipei de audit IT/auditorului IT persoană fizică/auditor IT intern certificat</td><td>Numele, prenumele, telefon, fax, adresa de e-mail şi adresa unde îşi desfăşoară activitatea</td></tr>
<tr><td>G</td><td>Semnătura coordonatorului certificat al echipei de audit şi semnătura reprezentantului legal al auditorului persoană juridică/semnătura auditorului IT persoană fizică/semnătura auditorului IT intern certificat</td><td rowspan="3"></td></tr>
<tr><td>H</td><td>Obiectivele activităţii de audit IT, perioada auditată</td></tr>
<tr><td>I</td><td>Sediul desfăşurării activităţii de audit IT, data întocmirii raportului de audit IT</td></tr>
<tr><td>J</td><td>Descrierea ariei auditului IT</td><td>Adresa sediului unde a avut loc activitatea de audit IT (sediu central/sucursală/filială), data întocmirii raportului de audit IT

Identificarea sistemelor informatice importante utilizate de către entitate şi raportarea acestora conform tabelului de mai jos:
<table>
<tr><th>Nr.</th><th>Sistem informatic important*</th><th>Funcţia îndeplinită</th><th>Administrarea sistemului informatic important (internă/externalizată)</th><th>Inclus în scopul auditului IT</th></tr>
<tr><td colspan="5">Pentru sistemele informatice importante incluse în scopul auditului IT se vor menţiona următoarele:
- descrierea componentelor hardware ale sistemelor informatice importante utilizate;
- măsurile organizatorice: politicile aplicabile şi procedurile implementate;
- un sumar conţinând analiza riscurilor aferente activităţii, a posibilelor deficienţe ale sistemului informatic important auditat şi a măsurilor de reducere a riscurilor asociate, în baza controalelor</td></tr>
</table></td></tr>
</table>

		generale sau specifice implementate conform prevederilor prezentei norme
K	Referiri cu privire la implementarea planului de acţiune asumat de entitate rezultat în urma activităţii de audit IT anterioare, dacă este cazul	Verificarea modului de implementare a măsurilor şi respectarea termenelor asumate
L	Referiri cu privire la veridicitatea indicatorilor raportaţi în conformitate cu prevederile art. 49 alin. (1) din prezenta normă, aferenţi perioadei dintre două activităţi de auditare IT şi conformitatea raportărilor efectuate către A.S.F.	
M	Referiri cu privire la modul de efectuare a evaluării anuale de către entitate a riscurilor operaţionale generate de utilizarea sistemelor informatice importante prevăzută la art. 6 alin. (1) din prezenta normă	Opinie cu privire la plauzibilitatea metodologiei/tehnicilor utilizate, precum şi asupra măsurilor de control implementate în vederea adresării riscurilor operaţionale identificate
N	Rezultatul obţinut în urma efectuării testului de penetrare, după caz	În situaţia efectuării testului de penetrare de către auditorul IT, se va menţiona: - descrierea metodologiei/tehnicilor utilizate; - menţionarea rezultatelor obţinute în urma testului; - recomandările adresate entităţii şi răspunsul managementului entităţii. În situaţia în care testul de penetrare nu a fost efectuat de către auditorul IT, acesta va verifica: - metodologia/tehnicile utilizate;

		- rezultatele obţinute în urma testului; - recomandările adresate entităţii şi răspunsul managementului entităţii.
O	Afirmaţia de conformitate, reflectată prin opinia auditorului IT	Opinie pozitivă, opinie cu rezerve/calificată, opinie negativă, după caz

II. Anexe la raportul de audit IT

1. Sumarul observaţiilor

Anexa este însuşită de către entitatea auditată prin semnarea acesteia către reprezentantul legal şi conţine, fără a se limita la acestea:

a) descrierea neconformităţii/constatării;

b) importanţa neconformităţii/constatării;

c) riscurile asociate;

d) probabilitatea ca aceste constatări să aibă un impact semnificativ; recomandările auditorului IT pentru acţiuni corective şi răspunsul conducerii entităţii auditate pentru fiecare constatare din raport (inclusiv în urma testului de penetrare);

e) planul de acţiune asumat de către entitatea auditată care conţine măsurile efective, termenul de implementare şi persoanele responsabile de implementare.

2. Analiza internă a riscurilor operaţionale şi registrul riscurilor

Anexa conţine următoarele informaţii, fără a se limita la acestea:

a) descrierea politicii/metodologiei utilizate de către entitate;

b) rezultatele revizuirii riscurilor generate de utilizarea sistemelor informatice;

c) rezultatele evaluării de către auditorul IT a măsurilor de control implementate în vederea adresării riscurilor operaţionale identificate (pentru riscuri semnificative).

3. Cerinţe referitoare la furnizorii externi şi furnizorii de servicii IT externalizate pentru sistemele informatice importante

Raportarea se efectuează prin completarea tabelului prezentat

Sistem informatic important	Funcţia sistemului informatic important - descrierea serviciilor oferite	Furnizor - date de identificare (denumire, sediul entităţii, datele de înregistrare fiscală, telefon/fax/website)	Certificare SR ISO/IEC 27001 sau echivalent (emitent, număr certificare, data emiterii, perioada de valabilitate)	Alte certificări în conformitate cu prevederile prezentei norme (emitent, număr certificare, data emiterii, perioada de valabilitate)	Concluzie - Conformitate Da/Nu/Parţial	Comentarii

4. Organizarea pe procese

Anexa cuprinde informaţii referitoare la managementul disponibilităţii, respectiv:

a) măsurarea disponibilităţii sistemelor informatice importante (conform cu cerinţele standardului TIA-942 tier 2);

b) sistemele informatice importante pentru care s-au efectuat măsurătorile cu privire la disponibilitatea acestora;

c) descrierea modului în care a fost efectuată măsurarea disponibilităţii sistemelor informatice importante.

Raportarea se efectuează prin completarea tabelului prezentat

Sistem informatic important	Disponibilitatea sistemului informatic important în perioada măsurată	Perioada supusă testării	Concluzie - Conformitate Da/Nu	Comentarii

5. Concluzii ale echipei de audit privind respectarea cerinţelor impuse

Nr.	Articol supus verificării	Conformitate DA/NU/PARŢIAL/ NEAPLICABIL	Comentarii/ Motivaţii în cazul nerespectării prevederii
1.	Art. 3 (3)		
2.	Art. 6 (1)		
3.	Art. 6 (2)		
4.	Art. 15 (1)		

5.	Art. 15 (2)		
6.	Art. 15 (3)		
7.	Art. 15 (4)		
8.	Art. 16 (1) - a)		
9.	Art. 16 (1) - b)		
10.	Art. 16 (1) - c)		
11.	Art. 16 (1) - d)		
12.	Art. 16 (1) - e)		
13.	Art. 16 (1) - f)		
14.	Art. 16 (1) - g)		
15.	Art. 16 (1) - h)		
16.	Art. 16 (2)		
17.	Art. 17 (1)		
18.	Art. 17 (2)		
19.	Art. 18 (1) - a)		
20.	Art. 18 (1) - b)		
21.	Art. 18 (1) - c)		
22.	Art. 18 (1) - d)		
23.	Art. 18 (1) - e)		
24.	Art. 19 - a)		
25.	Art. 19 - b)		
26.	Art. 19 - c)		
27.	Art. 19 - d)		
28.	Art. 20 - a)		
29.	Art. 20 - b)		
30.	Art. 20 - c)		
31.	Art. 20 - d)		

32.	Art. 35 (1) - a)		
33.	Art. 35 (1) - b)		
34.	Art. 35 (1) - c)		
35.	Art. 35 (2)		
36.	Art. 36 (1)		
37.	Art. 36 (2) - a)		
38.	Art. 36 (2) - b)		
39.	Art. 36 (2) - c)		
40.	Art. 36 (2) - d)		
41.	Art. 36 (2) - e)		
42.	Art. 36 (2) - f)		
43.	Art. 36 (2) - g)		
44.	Art. 36 (2) - h)		
45.	Art. 36 (2) - i)		
46.	Art. 37		
47.	Art. 45		
48.	Art. 46 (1) - a)		
49.	Art. 46 (1) - b)		
50.	Art. 46 (1) - c)		
51.	Art. 46 (1) - d)		
52.	Art. 46 (2)		
53.	Art. 47		
54.	Art. 48 - a)		
55.	Art. 48 - b)		
56.	Art. 48 - c)		

6. Declaraţia pe propria răspundere a auditorului IT extern

Anexa conţine informaţii cu privire la faptul că acesta nu se află în relaţii cu entitatea auditată, cu membrii structurii de conducere sau cu angajaţii acesteia care ar putea să îi afecteze independenţa sau obiectivitatea activităţii de audit IT.

7. Declaraţie pe propria răspundere a reprezentantului legal al entităţii auditate IT cu resurse interne

Anexa conţine informaţii cu privire la efectuarea auditului IT cu resurse interne certificate care sunt independente faţă de activitatea auditată şi copia certificatului de auditor IT semnată pentru conformitate cu originalul.

ANEXA Nr. 4

Indicatori de raportare electronică anuală

Pentru raportarea indicatorilor din tabelul de mai jos, entităţile vor raporta:

a) conform prevederilor art. 49 lit. c) din prezenta normă;

b) 0 "zero" - dacă nu sunt valori ale indicatorului respectiv pentru perioada raportată sau, după caz, la sfârşitul perioadei de raportare;

c) valoarea indicatorului - dacă sunt înregistrate valori diferite de zero ale indicatorului respectiv pentru perioada raportată sau, după caz, la sfârşitul perioadei de raportare.

Obiectiv în perioada de raportare	Indicator
1	2
Indicatori referitori la accesarea online a serviciilor oferite de entitate	
	Număr de clienţi (total utilizatori) care accesează serviciile online oferite de entitate
Indicatori referitori la persoanele care pot să efectueze modificări ale sistemelor/programelor informatice importante	
	Număr de persoane (total utilizatori) care au acces direct la bazele de date ale entităţii (referitor la portofolii, tranzacţii şi active) cu drepturi de modificare asupra acestora, rol de administrator sau privilegii echivalente
	Număr de persoane (total utilizatori) care au drepturi de modificare asupra programelor informatice importante ale entităţii (programe informatice interne/externe/online accesate via internet)
Indicatori referitori la principiul dublei validări prin operaţiuni în sistemele informatice importante	
	Număr de operaţiuni INIŢIATE care presupun dubla validare
	Număr de operaţiuni CONFIRMATE care presupun dubla validare
	Număr de operaţiuni ANULATE care presupun dubla validare
Indicatori referitori la accesul la sistemele informatice importante	

	Număr de persoane (total utilizatori) care au acces la sistemele informatice importante care conţin informaţii referitoare la portofolii, tranzacţii şi active
	Număr administratori de sistem (total utilizatori) care au acces la credenţialele conturilor de acces ale clienţilor
Indicatori referitori la incidente interne de securitate informatică, declarate	
	Număr total incidente interne de securitate informatică
	Număr total incidente informatice externe
	Număr încălcări politică şi proceduri securitate
	Număr pierderi date generate de acţiuni neaprobate
	Număr incidente declarate aferente pierderii de date (date electronice)
	Număr de incidente declarate care au dus la distrugere accidentală sau intenţionată de documente/înregistrări/fişiere
	Număr de incidente declarate de încălcare gravă a regulilor/fraude/înşelătorii
	Număr incidente declarate de distrugere în centrul de date
	Număr mediu de zile de la identificarea unui incident de securitate până la rezolvarea acestuia
Niveluri servicii agreate interne şi pentru clienţi	
	Număr de ore de indisponibilitate neprogramată a sistemelor informatice importante la care au acces clienţii (precum, dar nelimitat la aplicaţii de tranzacţionare online, aplicaţii online pentru subscrierea de poliţe de asigurare)
	Număr de ore de indisponibilitate neprogramată a serviciilor IT externalizate care afectează serviciile oferite către clienţii entităţilor
Management schimbări	
	Numărul programelor informatice importante
	Numărul de modificări aduse programelor informatice importante
	Număr erori în exploatare generate de deficienţe în proiectarea sistemelor informatice importante
	Număr erori în exploatare neidentificate în testarea sistemelor informatice importante
Indicatori managementul continuităţii	
	Număr de teste efectuate conform planului de continuitate a afacerii
	Număr de teste efectuate conform planului de recuperare în caz de dezastru
Audituri şi testări	
	Număr de audituri interne anuale