

NORMĂ nr. 4 din 28 februarie 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

EMITENT • **AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ**

Publicat în **MONITORUL OFICIAL nr. 233 din 16 martie 2018**

Data intrării în vigoare 15-04-2018

Formă consolidată valabilă la data 02-04-2020

Prezenta formă consolidată este valabilă începând cu data de 02-04-2020 până la data de 14-06-2020

Notă CTCE

Forma consolidată a **NORMEI nr. 4 din 28 februarie 2018**, publicate în Monitorul Oficial nr. 233 din 16 martie 2018, la data de 02 Aprilie 2020 este realizată prin includerea modificărilor și completărilor aduse de: **NORMA nr. 1 din 18 ianuarie 2019**; **NORMA nr. 21 din 1 aprilie 2020**.

Conținutul acestui act aparține exclusiv S.C. Centrul Teritorial de Calcul Electronic S.A. Piatra-Neamț și nu este un document cu caracter oficial, fiind destinat informării utilizatorilor.

În temeiul prevederilor **art. 3 alin. (1) lit. b)**, **art. 5, art. 6 alin. (2)** și ale **art. 14 din Ordonanța de urgență a Guvernului nr. 93/2012** privind înființarea, organizarea și funcționarea Autorității de Supraveghere Financiară, aprobată cu modificări și completări prin **Legea nr. 113/2013**, cu modificările și completările ulterioare, în urma deliberărilor Consiliului Autorității de Supraveghere Financiară din cadrul ședinței din data de 28 februarie 2018,

Autoritatea de Supraveghere Financiară emite prezenta normă.

Capitolul I Dispoziții generale

Articolul 1

(1) Prezenta normă stabilește cerințele la nivelul entităților autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară, denumită în continuare A.S.F., pentru identificarea, prevenirea și reducerea impactului potențial negativ al riscurilor operaționale generate de utilizarea tehnologiei informației și comunicațiilor la nivel de oameni, procese, sisteme și mediu extern, inclusiv pentru fapte ce țin de criminalitatea informatică.

(2) Prezenta normă reglementează activitățile și operațiunile pentru evaluarea, supravegherea și controlul riscurilor operaționale generate de utilizarea sistemelor informatice, precum și gestionarea riscurilor privind securitatea sistemelor informatice importante în vederea asigurării securității informatice a entităților prevăzute la **alin. (1)**.

Articolul 2

Prezenta normă se aplică următoarelor categorii de entități autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către A.S.F., denumite în continuare entități:

a) operatori de piață/operatori de sistem;
b) societăți de administrare a investițiilor (S.A.I.), administratori de fonduri de investiții alternative (A.F.I.A.), respectiv:

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

2. societăți care dețin 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/contrapărți centrale;

d) intermediari - societăți de servicii de investiții financiare (S.S.I.F.), sucursale ale intermediarilor din state terțe și instituții de credit din România autorizate de Banca Națională a României în conformitate cu legislația bancară și înscrise în Registrul A.S.F. în calitate de intermediar, respectiv:

La data de 30-01-2019 Partea introductivă a literei d) , Articolul 2 , Capitolul I a fost modificată de Punctul 1, Articolul I din NORMA nr. 1 din 18 ianuarie 2019, publicată în MONITORUL OFICIAL nr. 76 din 30 ianuarie 2019

1. intermediari care au calitatea de operatori independenți;

2. S.S.I.F. semnificative din punctul de vedere al mărimii, organizării interne și naturii, extinderii și complexității activității, conform reglementărilor specifice;

3. intermediari care prestează servicii conexe de păstrare în siguranță și administrare a instrumentelor financiare în contul clienților, inclusiv custodia și servicii în legătură cu aceasta, cum ar fi administrarea fondurilor sau garanțiilor;

4. intermediari care folosesc facilități de tranzacționare prin internet (ADP/AS) - platforme de preluare și transmitere a ordinelor clienților;
 5. intermediari care au calitatea de market makeri și/sau furnizori de lichiditate;
 6. intermediari care tranzacționează pe cont propriu și nu se încadrează în categoriile de la [pct. 1-5](#);
 7. intermediari care nu tranzacționează pe cont propriu și nu se încadrează în categoriile de la [pct. 1-5](#);
- e) Abrogată;

La data de 30-01-2019 Litera e) din Articolul 2 , Capitolul I a fost abrogată de Punctul 2, Articolul I din NORMA nr. 1 din 18 ianuarie 2019, publicată în MONITORUL OFICIAL nr. 76 din 30 ianuarie 2019

- f) Fondul de compensare a investitorilor, Fondul de garantare a asiguraților și Fondul de garantare a drepturilor din sistemul de pensii private;
 - g) societăți de asigurare și reasigurare;
 - h) intermediari principali care desfășoară activitate de distribuție a produselor de asigurare și reasigurare;
- La data de 30-01-2019 Litera h) din Articolul 2 , Capitolul I a fost modificată de Punctul 3, Articolul I din NORMA nr. 1 din 18 ianuarie 2019, publicată în MONITORUL OFICIAL nr. 76 din 30 ianuarie 2019
- i) Biroul asiguraților de autovehicule din România;
 - j) entități care desfășoară activitatea de depozitare a activelor organismelor de plasament colectiv și a fondurilor de pensii private;
 - k) administratorii fondurilor de pensii private.

Articolul 3

- (1) Entitățile prevăzute la [art. 2](#) au obligația de a identifica toate sistemele informatice importante utilizate pe ambele componente, respectiv infrastructura hardware și software, care sunt esențiale în activitatea desfășurată de către acestea.
- (2) Sistemele informatice importante prevăzute la [alin. \(1\)](#) cuprind, în funcție de tipul entității, cel puțin următoarele, fără a se limita la acestea:
 - a) sisteme informatice necesare pentru derularea în bune condiții a activității autorizate/avizate de A.S.F.:
 1. sisteme de tranzacționare/sisteme alternative de tranzacționare;
 2. sisteme de compensare, decontare, depozitare și custodie;
 3. platforme/aplicații de tranzacționare sau distribuție prin internet sau telefon;
 4. sisteme de gestiune asigurați;
 5. sisteme de gestiune și subscriere contracte de asigurare;
 6. sisteme de înregistrare și 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 participanților 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. aplicații online utilizate în scopul de distribuție și informare a clienților, 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. și alte instituții/entități ale pieței financiare;
 - c) sisteme informatice folosite în activitatea financiar-contabilă a entității, cum ar fi programele de contabilitate;
 - d) sisteme electronice de vot și alte sisteme informatice cu implicații semnificative asupra sistemului de guvernare al entității, precum sisteme de tip teleconferință/videoconferință utilizate pentru desfășurarea la distanță a ședințelor consiliului de administrație/consiliului de supraveghere;
 - e) sisteme informatice cu impact asupra planului pentru continuitatea afacerii și redresării activității în caz de dezastre;
 - f) aplicații centrale de business, altele decât cele care se încadrează la [lit. a\)-e\)](#);
 - g) infrastructura informatică utilizată pentru sistemele informatice importante găzduite în locațiile de centre de date.
- (3) Entitățile au obligația să întocmească și să actualizeze permanent un registru cu sistemele informatice importante identificate în conformitate cu prevederile [alin. \(1\)](#) și [\(2\)](#).
- (4) Registrul întocmit în conformitate cu prevederile [alin. \(3\)](#) este supus verificării de către auditorul IT.

Articolul 4

Entitățile extind scopul auditului IT și la alte sisteme în situațiile prevăzute la [art. 29 alin. \(1\)](#).

Articolul 5

(1) Prevederile prezentei norme se aplică de către entități în funcție de categoria de risc stabilită de către A.S.F. conform prevederilor [art. 10](#) și [11](#), precum și în funcție 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 funcție de natura, dimensiunea și complexitatea activității acesteia, precum și de riscurile pe care le poate induce și care au impact asupra activității.

Articolul 6

(1) Entitățile au obligația să evalueze anual și să monitorizeze continuu riscurile operaționale generate de utilizarea sistemelor informatice importante, să prioritizeze resursele, să implementeze măsuri de securitate informatică și 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 funcție de profilul de risc, de riscurile identificate, de incidentele apărute, în conformitate cu cerințele legale aplicabile.

Articolul 7

Entitățile participă la colectarea, analizarea, monitorizarea și raportarea evenimentelor de securitate informatică, în cadrul sistemului care va fi dezvoltat de către A.S.F.

Articolul 8

Termenii și expresiile utilizate în prezenta normă au înțelesul prevăzut în [anexa nr. 1](#).

Capitolul II

Încadrarea entităților în categorii de risc

Articolul 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.

Articolul 10

Încadrarea entităților prevăzute la [art. 2 lit. a\)-j\)](#) în categoriile de risc menționate la [art. 9](#) este următoarea:

- a) în categoria de risc major se încadrează entitățile prevăzute la [art. 2 lit. a\)](#), [lit. c\)](#), [lit. d\) pct. 1](#) și [lit. i\)](#);
- b) în categoria de risc important se încadrează entitățile prevăzute la [art. 2 lit. d\) pct. 2, 4 și 5](#), [lit. g\)](#) și [j\)](#);
- c) în categoria de risc mediu se încadrează entitățile prevăzute la [art. 2 lit. b\) pct. 1](#), [lit. d\) pct. 3](#) și [pct. 6](#) și [lit. f\)](#);
- d) în categoria de risc scăzut se încadrează entitățile prevăzute la [art. 2 lit. b\) pct. 2](#), [lit. d\) pct. 7](#) și [lit. h\)](#).

La data de 30-01-2019 Litera d) din Articolul 10, Capitolul II a fost modificată de Punctul 4, Articolul I din NORMA nr. 1 din 18 ianuarie 2019, publicată în MONITORUL OFICIAL nr. 76 din 30 ianuarie 2019

Articolul 11

Încadrarea entităților 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\)](#) și ale [art. 51 din Norma Autorității de Supraveghere Financiară nr. 3/2014](#) privind controlul intern, auditul intern și administrarea riscurilor în sistemul de pensii private.

Articolul 12

Încadrarea, respectiv reîncadrarea entităților menționate 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.

Articolul 13

Încadrarea, respectiv reîncadrarea entităților menționate la [art. 2 lit. d\)](#) se realizează în luna ianuarie a fiecărui an calendaristic, în baza activității autorizate de către A.S.F. și a deținerii calității de market maker/furnizor de lichiditate în ultima zi lucrătoare a anului anterior.

Articolul 14

Entitatea care prestează mai multe tipuri de activități autorizate de către A.S.F. și se încadrează în mai multe categorii de risc dintre cele prevăzute la [art. 9](#) respectă obligațiile pentru categoria de risc cea mai ridicată instituită de prezenta normă.

Capitolul III

Dispoziții privind activitățile obligatorii desfășurate de către entități

Articolul 15

(1) Entitățile au obligația să desfășoare cel puțin activitățile obligatorii corespunzătoare fiecărei categorii de risc prevăzute la [art. 9](#), conform tabelului din [anexa nr. 2](#).

(2) Entitățile au obligația ca, anual, să efectueze o scanare de vulnerabilități.

(3) Testele de penetrare regăsite în tabelul din anexa nr. 2 la lit. B) pct. 8 lit. c) au drept obiectiv 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.

(4) Entitățile au obligația să se asigure că în perioada supusă auditului IT sunt efectuate teste de penetrare externe, teste de penetrare interne și 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 și parametri privind modalitatea de implementare a activităților obligatorii prevăzute la [alin. \(1\)](#). Ghidul are un caracter orientativ și poate fi actualizat de către A.S.F. în funcție de bunele practici în domeniu.

Articolul 16

(1) Raportat la activitatea desfășurată, entitățile au obligația să se asigure că sistemele informatice importante utilizate îndeplinesc cel puțin următoarele cerințe:

a) asigură integritatea, confidențialitatea, autenticitatea, disponibilitatea datelor în concordanță cu categoria de risc a sistemului informatic important definită intern de către entitate, precum și prelucrarea acestora în conformitate cu reglementările A.S.F., luând în considerare posibilitatea actualizării acestora în funcție de modificările intervenite în legislația incidentă;

b) asigură respectarea conținutului de informații prevăzut în formularele de raportare, așa cum sunt prevăzute în legislația specifică, precum și alte raportări solicitate prin reglementările A.S.F.;

c) asigură stocarea și păstrarea datelor înregistrate și jurnalizate de către sistemele de tranzacționare, de emitere contracte de asigurări/avizare dosare de daune și sisteme back-office pentru o perioadă de timp în conformitate cu legislația aplicabilă în vigoare. Sistemul de păstrare a datelor trebuie să permită ca aceste date să poată fi transmise sau puse la dispoziția 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 și identificarea utilizatorilor sistemului în acel moment;

e) asigură confidențialitatea și protecția informațiilor și a programelor prin parole, coduri de identificare pentru accesul la informații, precum și realizarea de copii de siguranță pentru programele și informațiile deținute;

f) asigură mecanisme de securitate și control al sistemelor informatice importante, pentru păstrarea în siguranță a datelor și informațiilor stocate, a fișierelor și bazelor de date, inclusiv în situația unor incidente;

g) asigură reconstituirea rapoartelor și informațiilor supuse verificării;

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

(2) Entitățile au obligația să se asigure că sunt îndeplinite următoarele cerințe:

a) nu există posibilitatea autentificării multiple a mai multor persoane pe același cont de aplicație;

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

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

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

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

f) să se asigure că utilizatorii autorizați nu furnizează elementele de autentificare către terțe persoane.

Articolul 17

(1) Entitățile au obligația 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 și să acopere toate sistemele informatice și rețelele utilizate de către entitate.

Articolul 18

(1) Entitățile au obligația 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 informații, 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 și externe pe toată durata testării;

c) cauzele și impactul real/potențial al incidentului de securitate informatică asupra datelor entității;

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

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

(2) Raportul de testare prevăzut la [alin. \(1\)](#) este păstrat la sediul entității care are obligația să îl prezinte auditorului IT și A.S.F. la solicitarea acestuia.

Articolul 19

Sistemele informatice importante care oferă intermediarilor și clienților acestora accesul la platforme electronice de tranzacționare, precum și sistemele informatice importante care evidențiază operațiuni de compensare, decontare și registru pentru instrumente financiare și operațiuni cu aceste instrumente, asigură, fără a se limita la acestea:

- a)** securitatea și integritatea datelor procesate prin folosirea unei modalități de securizare atât asupra datelor trimise către platformele electronice de tranzacționare și către cele de compensare, decontare și registru, cât și asupra datelor recepționate de la aceste platforme;
- b)** mecanisme care să garanteze nerepudierea datelor transmise și recepționate;
- c)** jurnalizarea în timp real a informației despre ordinele transmise spre executare, a stării acestor ordine, respectiv a modificărilor care se aduc acestor ordine în decursul existenței lor de către clienții și intermediarii care utilizează aceste sisteme informatice importante;
- d)** mecanisme de nerepudiare a integrității înregistrării operațiunilor de sistem informatic important.

Articolul 20

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

- a)** securitatea și integritatea datelor procesate prin folosirea unei modalități de securizare asupra datelor trimise către platformele electronice de distribuire a titlurilor de participare;
- b)** mecanisme care să garanteze nerepudierea datelor transmise și recepționate;
- c)** jurnalizarea în timp real a informației despre instrucțiunile investitorilor transmise către S.A.I./A.F.I.A.;
- d)** mecanisme de nerepudiare a integrității înregistrării operațiunilor de sistem informatic.

Capitolul IV

Auditarea și testarea sistemelor informatice importante

Secțiunea 1

Dispoziții privind auditul IT

Articolul 21

(1) Entitățile au obligația de a audita sistemele informatice importante, după cum urmează:

- a)** entitățile încadrate în categoria de risc major au obligația 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 sfârșitului perioadei supuse auditului IT anterior;
- b)** entitățile încadrate în categoria de risc important au obligația 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 sfârșitului perioadei supuse auditului IT anterior;
- c)** entitățile încadrate în categoria de risc mediu au obligația 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 sfârșitului perioadei supuse auditului IT anterior;
- d)** entitățile încadrate în categoria de risc scăzut au obligația 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 sfârșitului perioadei supuse auditului IT anterior.

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

Articolul 22

Entitățile care efectuează auditul IT cu resurse interne certificate au obligația să utilizeze personal certificat în domeniul auditării IT, angajat în cadrul entității sau în cadrul unei companii din cadrul aceluiași grup financiar, cu respectarea prevederilor prezentei norme și a metodologiilor certificate internațional.

Articolul 23

(1) Auditul IT extern se efectuează în baza unui contract de audit IT încheiat între entitatea care a solicitat auditarea și un auditor IT extern înscris în Lista auditorilor IT externi menținută de A.S.F. în conformitate cu prevederile [art. 38](#).

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

Articolul 24

Entitatea are obligația 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 cerințele impuse pentru efectuarea auditului sistemelor informatice importante, în conformitate cu prevederile prezentei norme și cu bunele practici în domeniu.

Articolul 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 și care:

- a) este de natură să afecteze continuitatea activității entității 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.

Articolul 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 cunoștința entității auditate;
- b) o declarație care să indice motivele de încetare a contractului de audit IT, indiferent de natura acestora;
- c) orice alte informații sau documente solicitate în legătură cu activitatea de audit IT extern.

Articolul 27

Auditorul IT care efectuează activitatea de audit IT la entitățile prevăzute la [art. 2](#) are obligația de a întocmi și de a prezenta conducerii entității o situație a deficiențelor și vulnerabilităților identificate.

Articolul 28

La finalizarea auditului IT, auditorii IT au obligația de a întocmi un raport de audit IT însoțit de anexe, care să cuprindă cel puțin elementele prevăzute în macheta de raportare prezentată în [anexa nr. 3](#), dar fără a se limita la acestea.

Articolul 29

- (1) A.S.F. poate să instituie în sarcina entității obligația de a audita IT orice sisteme informatice dacă:
 - a) în urma constatărilor rezultă că entitatea nu a desfășurat toate activitățile minime obligatorii categoriei de risc în care aceasta a fost încadrată, conform prevederilor [art. 10](#) sau 11, sau activitățile desfășurate au un caracter formal;
 - b) apreciază că se impune efectuarea unor investigații suplimentare la nivelul sistemelor informatice.
- (2) Instituirea de către A.S.F. a obligației de a audita IT alte sisteme informatice conform [alin. \(1\)](#) cuprinde și termenul până la care entitatea este obligată să transmită la A.S.F. raportul de audit, iar acest termen nu poate să depășească 90 de zile de la data instituirii obligației de a audita alte sisteme informatice de către A.S.F.

Articolul 30

Entitățile, 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 desfășurarea activității de audit IT.

Articolul 31

Entitățile, inclusiv cele care efectuează auditul IT cu resurse interne certificate, sunt obligate să se asigure că activitatea de audit IT este independentă față de activitatea auditată, pentru a nu fi compromisă obiectivitatea acesteia, iar auditorii IT sunt independenți și obiectivi în toate aspectele legate de activitatea de audit IT.

Articolul 32

În aplicarea prevederilor [art. 31](#), entitățile 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 și care este de natură să afecteze continuitatea activității entității 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 cunoștința entității auditate sau orice alte informații ori documente solicitate în legătură cu activitatea de audit IT.

Articolul 33

Entitățile, inclusiv cele care efectuează auditul IT cu resurse interne certificate, sunt obligate să furnizeze auditorului IT informații complete, corespunzătoare, relevante și în timp util, pentru a permite desfășurarea în bune condiții a activității de audit IT.

Articolul 34

Respectarea prevederilor [art. 25](#) și [26](#) nu contravine conduitei etice și profesionale, nu constituie o încălcare a secretului profesional impus prin clauze contractuale sau prin prevederi legale și nu atrage niciun fel de răspundere asupra persoanei fizice și/sau juridice în cauză.

Secțiunea a 2-a

Testarea sistemelor informatice importante

Articolul 35

(1) Entitatea are obligația de a ține evidența 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 situația dezafectării unui sistem informatic important, entitatea are obligația să solicite efectuarea unui audit IT cu resurse interne certificate sau externe care vizează sistemele ce urmează a fi dezafectate.

Articolul 36

(1) Entitatea are obligația să testeze sistemele informatice importante înainte de prima utilizare și la orice modificare în cadrul ciclului de viață 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 aplicațiilor utilizate și a persoanelor implicate;
- f) analiza riscurilor implicate de achiziția sau modificarea programului informatic, a posibilelor vulnerabilități și 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 și rezultatul testării;
- h) concluzia echipei de testare;
- i) semnătura membrilor echipei de testare.

Articolul 37

Entitatea are obligația să păstreze rapoartele de testare IT pentru o perioadă de cel puțin 5 ani după momentul dezafectării sistemului informatic important și să le pună la dispoziția A.S.F. sau auditorului IT, la cerere.

Capitolul V

Înscrierea auditorul IT extern

Articolul 38

Auditorul IT extern care intenționează să presteze servicii de audit IT pentru entitățile cărora le sunt incidente prevederile prezentei norme are obligația înscrierii în Lista auditorilor IT externi menționată de A.S.F.

Articolul 39

În vederea înscrierii în lista prevăzută la [art. 38](#), auditorul IT extern depune la A.S.F. o cerere, în care menționează sectorul/sectoarele în care activează entitățile pentru care intenționează să presteze servicii de audit IT, însoțită de documentația care trebuie să cuprindă următoarele, după caz:

- a) datele de identificare ale auditorului IT extern:
 - 1. numele complet/denumirea și adresa/sediul - adresa completă;
 - 2. adresa unde își desfășoară activitatea;
 - 3. telefon/fax, e-mail, adresa paginii de internet;
- b) pentru auditorul IT persoană fizică certificată și reprezentantul societății 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 și semnat, cu prezentarea experienței profesionale în auditarea IT externă a sistemelor informatice;
 - 3. certificatul de auditor IT, în copie, semnată pentru conformitate cu originalul, din care reiese experiența în domeniul de audit IT extern al sistemelor informatice;
 - 4. dovada experienței și a specializării pe domeniul de audit IT extern al sistemelor informatice;
 - 5. certificat constatator emis de Oficiul Național al Registrului Comerțului, cu starea la zi a persoanei juridice, în original;
 - 6. certificatul de cazier judiciar și 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 documentației, în copie;

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

Articolul 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.

Articolul 41

Orice modificare a documentației prevăzute la [art. 39 lit. b\) pct. 1, 3, 5, 6 și 7](#) trebuie transmisă A.S.F. în termen de maximum 30 de zile de la data efectuării modificării.

Articolul 42

A.S.F. radiază din lista prevăzută la [art. 38](#) auditorii IT externi în oricare dintre următoarele situații:

- a) la cererea acestora;
- b) în cazul lichidării sau la declanșarea insolvenței;
- c) în cazul încălcării prevederilor [art. 25, 26, 28 și 41](#);
- d) în cazul nerespectării prevederilor prezentei norme.

Articolul 43

Pentru toate situațiile menționate la [art. 42 lit. c\)](#) și [d\)](#), A.S.F. transmite auditorului IT extern o notificare prealabilă prin care i se aduc la cunoștință faptele pentru care A.S.F. va proceda la inițierea demersurilor pentru radierea din Lista auditorilor IT externi.

Capitolul VI

Dispoziții privind furnizorii externi și furnizorii de servicii IT externalizate pentru sistemele informatice importante

Articolul 44

Orice externalizare de servicii se realizează cu respectarea legislației aplicabile entității.

Articolul 45

În situațiile în care entității nu îi sunt aplicabile alte prevederi legale referitoare la externalizarea unor servicii IT și în toate cazurile în care sunt utilizate serviciile unor furnizori externi, pentru toate sistemele informatice importante, entitatea are obligația 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.

Articolul 46

(1) Notificarea prevăzută la [art. 45](#) trebuie să conțină următoarele informații și documente, după caz:

- a) descrierea serviciilor furnizate/externalizate;
 - b) datele de identificare a furnizorului:
 - 1. sediul societății - adresa completă;
 - 2. telefon/fax, e-mail, pagina de internet;
 - c) certificat constatator emis de Oficiul Național al Registrului Comerțului, cu starea la zi a persoanei juridice, sau echivalentul acestuia pentru furnizorii externi înregistrați în alte state, în original sau copii conforme cu originalul;
 - d) documente în funcție de tipul serviciului sau activității desfășurate, astfel:
 - 1. SR ISO/IEC 27001 sau certificări pentru standarde echivalente - pentru toți furnizorii;
 - 2. certificări pentru furnizarea și dezvoltarea de programe informatice software;
 - 3. certificări pentru furnizarea de servicii externalizate;
 - 4. act doveditor privind respectarea condițiilor 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 activităților externalizate pentru furnizarea de servicii externalizate de tip cloudcomputing public.
- (2) Certificările prevăzute la [alin. \(1\) lit. d\) pct. 1, 2, 3 și 6](#) trebuie să fie emise de entități/organisme abilitate /recunoscute pe plan intern și/sau internațional.

Articolul 47

Entitatea are obligația ca, în cazul modificării unor informații și/sau documente prevăzute la [art. 46](#), care pot conduce la afectarea desfășurării serviciilor externalizate conform contractului, să notifice A.S.F. și să depună originalul sau copia documentelor modificate în termen de maximum 90 de zile de la data efectuării modificării.

Articolul 48

Pentru sistemele informatice importante, entitatea are obligația să se asigure că furnizorii de servicii IT externalizate, inclusiv în cazul externalizărilor în lanț, cu excepția furnizorilor de servicii de comunicații, de hardware sau de licențe software, raportat strict la activitatea externalizată:

- a) permit respectarea de către entitate a prevederilor prezentei norme, astfel încât prin externalizarea anumitor activități să nu se încalce legislația aplicabilă;
- b) prezintă, la solicitarea A.S.F., modalitatea prin care sunt îndeplinite de către entitate prevederile prezentei norme;
- c) permit A.S.F. și auditorului IT să verifice și/sau să auditeze sistemele sale informatice în contextul aplicării prevederilor prezentei norme sau pun la dispoziția auditorului IT un raport de audit IT întocmit în conformitate cu standardele ISAE 3402 sau echivalent pentru sistemele informatice puse la dispoziția entității.

Capitolul VII

Dispoziții privind raportarea

Articolul 49

Entitatea are obligația să întocmească în conformitate cu prevederile prezentei norme și ale altor reglementări incidente și să transmită A.S.F. următoarele rapoarte:

- a) raportul anual privind evaluarea internă a riscurilor operaționale 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, însoțit de copia certificatului de auditor IT semnată pentru conformitate cu originalul valabil la momentul întocmirii raportului de audit;

Notă

Conform [alin. \(2\) al art. 2 din NORMA nr. 21 din 1 aprilie 2020](#), publicată în MONITORUL OFICIAL nr. 277 din 02 aprilie 2020, termenul prevăzut la [art. 49 lit. b\) din Norma Autorității de Supraveghere Financiară 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, 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 menționați în [anexa nr. 4](#), în cazul în care acești indicatori sunt aplicabili și sunt aferenți sistemelor informatice importante, până la data de 31 martie a anului curent, pentru anul anterior.

Articolul 50

În cazul în care au fost identificate deficiențe/ vulnerabilități în conformitate cu prevederile [art. 27](#), raportul de audit IT prevăzut la [art. 49 lit. b\)](#) se transmite A.S.F. însoțit de planul de acțiune din care să rezulte modalitatea de remediere a deficiențelor/vulnerabilităților identificate de auditorul IT.

Articolul 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 atribuții de supraveghere, pe suport hârtie sau în format electronic cu semnătură electronică extinsă, după caz.

Capitolul VIII

Dispoziții tranzitorii și finale

Articolul 52

Nerespectarea prevederilor prezentei norme de către entitățile prevăzute la [art. 2](#) constituie contravenție conform prevederilor Legii nr. 236/2018 privind distribuția de asigurări, ale Legii nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, cu modificările și completările ulterioare, ale Legii nr. 297/2004 privind piața de capital, cu modificările și completările ulterioare, ale Ordonanței de urgență a Guvernului nr. 32 /2012 privind organismele de plasament colectiv în valori mobiliare și societățile de administrare a investițiilor, precum și pentru modificarea și completarea Legii nr. 297/2004 privind piața de capital, aprobată cu modificări și completări prin Legea nr. 10/2015, cu modificările și completările ulterioare, ale Legii nr. 74/2015 privind administratorii de fonduri de investiții alternative, cu modificările și completările ulterioare, ale Legii nr. 126/2018 privind piețele de instrumente financiare, ale Legii nr. 411/2004 privind fondurile de pensii administrate privat, republicată, cu modificările și completările ulterioare, ale Legii nr. 204/2006 privind pensiile facultative, cu modificările și completările ulterioare, ale Legii nr. 187/2011 privind înființarea, organizarea și funcționarea Fondului de garantare a drepturilor din sistemul de pensii private, ale Legii nr. 213/2015 privind Fondul de garantare a asiguraților și ale Legii nr. 132/2017 privind asigurarea obligatorie de răspundere civilă auto pentru prejudicii produse terților prin accidente de vehicule și tramvaie

La data de 30-01-2019 Articolul 52 din Capitolul VIII a fost modificat de Punctul 5, Articolul I din NORMA nr. 1 din 18 ianuarie 2019, publicată în MONITORUL OFICIAL nr. 76 din 30 ianuarie 2019

Articolul 53

- (1) Începând cu anul 2018, entitățile au obligația 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](#).

Articolul 54

- (1) Prevederile prezentei norme se aplică entităților 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 desfășurare la data intrării în vigoare a prezentei norme va continua în conformitate cu reglementările în vigoare la data începerii auditului IT.

Articolul 55

[Anexele nr. 1-4](#) fac parte integrantă din prezenta normă.

Articolul 56

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

Articolul 57

La data intrării în vigoare a prezentei norme se abrogă [Norma Autorității de Supraveghere Financiară nr. 6/2015](#) privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate și/sau supravegheate de Autoritatea de Supraveghere Financiară, publicată în Monitorul Oficial al României, Partea I, nr. 227 din 3 aprilie 2015, cu modificările și completările ulterioare.

Președintele Autorității de Supraveghere Financiară,

Leonardo Badea

București, 28 februarie 2018.

Nr. 4.

Anexa nr. 1

Definiții și abrevieri

1. arhivare electronică - stocarea documentelor în format digital;
2. analiză de risc - analiza scenariilor de amenințări semnificative, pentru a evalua probabilitatea materializării acestora și impactul potențial pe care un astfel de eveniment l-ar avea asupra entității și operațiunilor acesteia;
3. atac etic/test de penetrare - test al sistemelor informatice realizat printr-o simulare a unui atac real asupra rețelelor, sistemelor și programelor informatice utilizate de entitatea testată sau auditată, după caz;
4. audit IT - activitatea de colectare și evaluare a unor probe pentru a determina dacă sistemul informatic respectă parametrii de performanțe și de lucru conform cerințelor de proiectare, dacă asigură funcționalitățile necesare cerințelor de afaceri și respectarea legislației în domeniu, dacă este securizat, dacă menține integritatea datelor prelucrate și stocate, dacă permite atingerea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;
5. auditor IT - persoana fizică autorizată care deține certificat de auditor IT sau persoană juridică cu personal certificat, care derulează o activitate de auditare a sistemelor informatice, conform reglementărilor și bunelor practici în domeniu;
6. bază de date - structură de organizare a informației în unul sau mai multe domenii de aplicare, cu scopul de a o face accesibilă în permanență către utilizatori prin ansamblul de programe informatice;
7. centru de date - spațiu securizat, dotat cu tehnică de calcul și echipamente de comunicații prin intermediul cărora se primesc, se stochează și 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 îndeplinește cerințele TIA-942 tier 2 sau echivalent și a cărui infrastructură prezintă caracteristicile de disponibilitate de 99,741%, circuit dedicat pentru răcire și alimentare cu energie electrică, include componente redundante, include podea înălțată, surse neîntreruptibile de putere, generator și se încadrează într-un număr de maximum 22 de ore de nefuncționare pe an;

- 9.** ciclul de viață - totalitatea stadiilor din viața unui serviciu IT, a unui element de configurație, 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 și este asigurată prin centre de date publice, altele decât infrastructura informatică proprie entității, prin intermediul unui furnizor extern, ca un ansamblu distribuit de servicii de calcul, programe informatice, acces la informații și stocare de date;
- 11.** comunicații/telecomunicații - sisteme de transmisie, precum și orice alte resurse care permit transportul semnalelor prin fir, radio, fibră optică sau orice alte mijloace electromagnetice, precum și tehnologiile utilizate în cadrul proceselor de comunicare, care presupun existența unui mediu informatic constituit din echipamente hardware, software specializat, precum și dispozitive electronice de transmisie/ recepție date;
- 12.** controale informatice - totalitatea politicilor, procedurilor, practicilor și a structurilor organizaționale informatice proiectate să ofere o asigurare rezonabilă asupra faptului că obiectivele afacerii vor fi atinse și evenimentele nedorite vor fi prevenite sau detectate și corectate;
- 13.** date (informatice) - orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic, incluzându-se și orice program informatic care poate determina realizarea unei funcții similare de către un sistem informatic;
- 14.** disponibilitate - capacitatea unui serviciu IT sau unui element de configurație IT de a efectua funcțiile agreate atunci când este necesar acest lucru;
- 15.** dubla validare/validare dublă - validarea unei acțiuni de către doi utilizatori sau existența unei validări informatice duble ce implică un program care verifică o anumită acțiune prin metode diferite;
- 16.** externalizare servicii IT - utilizarea de către o entitate a unui furnizor extern de servicii IT, în vederea desfășurării de către acesta, pe bază contractuală și în mod continuu sau pentru o perioadă, a operațiunilor aferente suportului tehnic sau al procesării, necesare desfășurării activității efectuate în mod obișnuit de către entitatea în cauză;
- 17.** externalizare în lanț - externalizare în cadrul căreia furnizorul extern subcontractează cu alți furnizori externi elemente componente ale serviciilor prestate entității;
- 18.** furnizor extern - persoană juridică sau fizică autorizată furnizoare de bunuri (precum hardware, licențe software, componente etc.) și soluții informatice, care deține 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 și expertiză în domeniul serviciilor informatice, furnizoare de servicii informatice în condițiile respectării cadrului legal aplicabil și a autorizării primite;
- 20.** hardware - ansamblul elementelor fizice și tehnice cu ajutorul cărora datele se pot culege, verifica, prelucra, transmite, afișa și stoca, inclusiv suporturile de memorare a datelor, precum și echipamentele de calculator auxiliare;
- 21.** incident de securitate - eveniment înregistrat și declarat la nivelul entității privind securitatea informației sau a sistemelor informatice cu o probabilitate semnificativă de compromitere a operațiunilor și de amenințare a securității IT a cărei consecință a determinat sau este de natură să determine compromiterea informațiilor sau a sistemelor informatice;
- 22.** indicatori-cheie de performanță (KPI) - parametri analitici reprezentativi selectați pentru monitorizarea unor activități și procese-cheie pentru entități, oferind o privire de ansamblu asupra performanței;
- 23.** indicatori-cheie de risc (KRI) - parametri care măsoară efectiv riscurile aferente procedurilor și activităților entității, furnizând în timp semnalări corespunzătoare ale consecințelor cu efect negativ, care pot genera potențiale 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/importanță a serviciului nu este disponibilă;
- 25.** informație - rezultatul prelucrării datelor printr-un sistem informatic care sunt baza pentru asigurarea cunoașterii prin intermediul unor elemente noi în raport cu cunoștințele anterioare și constituie o resursă care trebuie protejată;
- 26.** infrastructura informatică - elemente ale bazei tehnico-materiale, pe componente sau ca sistem, care susțin culegerea, stocarea și managementul datelor, precum și integrarea, căutarea și vizualizarea datelor și alte calcule și servicii de procesare a informației utilizând tehnologii informatice, deținute sau contractate extern de către entitate și necesare bunei funcționări a acesteia;
- 27.** integritate - păstrarea datelor electronice, digitalizate, nealterate pe timpul comunicației dintre corespondenți sau pe perioada de stocare a datelor;
- 28.** ISACA - Asociația de Audit și Control al Sistemelor Informatice/Information Systems Audit and Control Association;

- 29.** ISAE 3402 - standard de audit utilizat pentru obținerea unor rapoarte de asigurare privind controalele din cadrul unei organizații prestatoare de servicii;
- 30.** SR ISO/IEC 27001 - standard care stabilește cerințele pentru un sistem de management al securității informației;
- 31.** managementul schimbării - procesul responsabil cu controlul ciclului de viață al tuturor schimbărilor pentru a permite implementarea schimbărilor benefice cu minimum de întrerupere a serviciilor IT;
- 32.** nerepudiere - atribut care să prevină posibilitatea unei entități de a nega o acțiune întreprinsă în context informațional;
- 33.** plan de cooperare în domeniul securității rețelelor și a informației - plan care stabilește rolurile organizaționale, obligațiile și răspunderile în cadrul cooperării, precum și procedurile de menținere sau de restabilire a funcționării rețelelor și sistemelor informatice în cazul în care acestea sunt afectate de un risc sau de un incident cibernetic cu impact semnificativ;
- 34.** program informatic (aplicație) - ansamblu de instrucțiuni care poate fi executat de un sistem informatic în vederea obținerii unui rezultat determinat;
- 35.** resurse informaționale - totalitatea informațiilor și a documentelor, conform cerințelor stabilite de legislația în domeniu; utilizat doar în definiția auditului IT;
- 36.** rețea - ansamblu de echipamente legate între ele prin canale de transmisie, precum, dar fără a se limita la, o rețea de calculatoare;
- 37.** risc de securitate - orice circumstanță sau eveniment care are un efect negativ potențial asupra securității sistemelor informatice;
- 38.** risc sistemic - riscul de afectare a unei zone importante a sistemului financiar sau a unei piețe financiare, cu potențial de consecințe negative serioase pentru piața internă și economia reală, instabilitate a sistemului financiar, posibil catastrofică, cauzată sau accentuată de evenimente idiosincratice sau de condiții ale entităților;
- 39.** riscuri semnificative - riscuri cu impact însemnat asupra situației financiare, patrimoniale și/sau reputaționale a entităților;
- 40.** raport de audit IT - instrumentul prin care se comunică scopul auditării, obiectivele urmărite, normele /standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările și concluziile auditului, precum și 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 și concluziile testării, precum și orice rezervă pe care echipa de testare o are asupra sistemului informatic testat;
- 42.** risc aferent tehnologiei informației (IT) - subcomponentă a riscului operațional care se referă la riscul actual sau viitor de afectare negativă, pe de o parte, a profiturilor și capitalului entităților sau a investitorilor, participanților sau asiguraților, pe de altă parte, determinat de inadecvarea strategiei și politicilor IT, a tehnologiei informației și a procesării acesteia, din punctul de vedere al capacității de gestionare, integritate, controlabilitate și continuitate, sau de utilizare necorespunzătoare a tehnologiei informației;
- 43.** securitate (cibernetică) - capacitatea unei rețele sau a unui sistem informatic, rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive, de a rezista, la un nivel de încredere dat, unei acțiuni accidentale sau răuvoitoare care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de rețeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;
- 44.** semnătură electronică (digitală) - atribut indispensabil al documentului electronic, obținut în urma transformării criptografice a acestuia, cu utilizarea cheii private, conform prevederilor [Legii nr. 455/2001](#) privind semnătura electronică, republicată;
- 45.** serviciu IT - combinație de persoane, procese și tehnologii furnizate în interiorul entității sau de către un furnizor de servicii IT, care se bazează pe folosirea tehnologiei informației și care asigură suportul tehnic necesar desfășurării activității entității și care ar trebui să fie definită într-un acord al nivelului agreeat de serviciu (SLA);
- 46.** sistem informatic - ansamblu de elemente intercorelate funcțional în scopul automatizării obținerii informațiilor necesare activităților operaționale și manageriale într-o entitate, prin intermediul serviciilor IT, al echipamentelor hardware și produselor software, proceduri manuale, baze de date și modele matematice pentru analiză, planificare, control și luarea deciziilor, utilizând componente de introducere și prelucrare date, componente de procesare precum servere, calculatoare, sisteme software de operare de bază, programe informatice, rețele de calculatoare și telecomunicații, componente de stocare și utilizatori, fără ca enumerarea să fie limitativă;
- 47.** software - toată gama de produse program, care cuprinde cel puțin următoarele elemente: sisteme de operare, drivere sau programe informatice;
- 48.** tehnologia informației (IT) sau tehnologia informației și a comunicațiilor - tehnologia necesară pentru prelucrarea (procurarea, procesarea, stocarea, convertirea și transmiterea) informației, în particular prin folosirea calculatoarelor electronice și a programelor corespunzătoare;

49. TIA-942 - standard ce definește infrastructura unui centru de date, în mod special din privința sistemului de cablare și a designului rețelei, dar acoperă și locația, răcirea, alimentarea cu energie electrică și amenajarea sa, precum și considerente legate de mediu;

50. vulnerabilități - stări de fapt, procese și/sau fenomene care diminuează capacitatea de reacție a sistemelor informatice la riscurile existente ori potențiale sau care favorizează apariția și dezvoltarea lor, cu consecințe în planul funcționalității și utilității.

Anexa nr. 2

Activități obligatorii desfășurate de către entități

Entitățile vor desfășura activitățile precizate în tabelul de mai jos, conform categoriilor de risc corespunzătoare.

Activități obligatorii ale entităților, pe categorii de risc

	Activitate	Categorii de risc a entității			
		Majoră	Importantă	Medie	Scăzută
A.	Evaluare internă a riscului operațional și 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 viață 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 configurații	x	x		
7	Management niveluri servicii (SLA)	x	x	x	
8	Management securitate				
a)	Cerințe generale	x	x	x	x
b)	Scanare de vulnerabilități	x	x	x	x
c)	Teste de penetrare ¹	x	x	x	
9	Management continuitate	x	x	x	
C.	Puncte de control și 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 performanță (KPI)	x			
E.	Implementare indicatori-cheie de risc (KRI)	x	x		
F.	Managementul securității 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

Notă

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 observațiilor

2. Analiza internă a riscurilor operaționale și registrul riscurilor

3. Cerințe referitoare la furnizorii externi și furnizorii de servicii IT externalizate pentru sistemele informatice importante

4. Organizarea pe procese

5. Concluzii ale echipei de audit privind respectarea cerințelor impuse

6. Declarația pe propria răspundere a auditorului IT extern

7. Declarație pe propria răspundere a reprezentantului legal al entității auditate IT cu resurse interne

I. Raportul de audit IT

#	Capitol	Comentarii/Explicații																														
A	Titlul raportului																															
B	Destinatarii raportului și orice restricții privind conținutul și circulația raportului																															
C	Paragraf introductiv	Identificarea entității auditate (Denumire/Numărul de înregistrare la Oficiul Național al Registrului Comerțului/Adresă) Includerea afirmației că sistemele informatice au fost auditate ca urmare a obligației legale impuse de prezenta normă																														
D	Asumarea responsabilității conducerii entității privind auditul efectuat asupra sistemelor informatice																															
E	Responsabilitatea auditorului IT	Raportul de audit IT va include cel puțin afirmațiile: - 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 ... (menționarea acestuia)																														
F	Datele de identificare ale coordonatorului certificat al echipei de audit IT/auditorului IT persoană fizică/auditor IT intern certificat	Numele, prenumele, telefon, fax, adresa de e-mail și adresa unde își desfășoară activitatea																														
G	Semnătura coordonatorului certificat al echipei de audit și semnătura reprezentantului legal al auditorului persoană juridică/semnătura auditorului IT persoană fizică/semnătura auditorului IT intern certificat																															
H	Obiectivele activității de audit IT, perioada auditată																															
I	Sediul desfășurării activității de audit IT, data întocmirii raportului de audit IT	Adresa sediului unde a avut loc activitatea de audit IT (sediul central/sucursală/filială), data întocmirii raportului de audit IT																														
J	Descrierea ariei auditului IT	Identificarea sistemelor informatice importante utilizate de către entitate și raportarea acestora conform tabelului de mai jos: <table border="1" data-bbox="635 1357 1181 1608"> <thead> <tr> <th>Nr.</th> <th>Sistem informatic important*)</th> <th>Funcția îndeplinită</th> <th>Administrarea sistemului informatic important (internă/externalizată)</th> <th>Inclus în scopul auditului IT</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table> Pentru sistemele informatice importante incluse în scopul auditului IT se vor menționa următoarele: - descrierea componentelor hardware ale sistemelor informatice importante utilizate; - măsurile organizatorice: politicile aplicabile și procedurile implementate; - un sumar conținând analiza riscurilor aferente activității, a posibilelor deficiențe ale sistemului informatic important auditat și a măsurilor de reducere a riscurilor asociate, în baza controalelor generale sau specifice implementate conform prevederilor prezentei norme	Nr.	Sistem informatic important*)	Funcția îndeplinită	Administrarea sistemului informatic important (internă/externalizată)	Inclus în scopul auditului IT																									
Nr.	Sistem informatic important*)	Funcția îndeplinită	Administrarea sistemului informatic important (internă/externalizată)	Inclus în scopul auditului IT																												
K	Referiri cu privire la implementarea planului de acțiune asumat de entitate rezultat în urma activității de audit IT anterioare, dacă este cazul	Verificarea modului de implementare a măsurilor și respectarea termenelor asumate																														
L	Referiri cu privire la veridicitatea indicatorilor raportați în conformitate cu prevederile art. 49 alin. (1) din prezenta normă, aferenți perioadei dintre două																															

	activități de auditare IT și conformitatea raportărilor efectuate către A.S.F.	
M	Referiri cu privire la modul de efectuare a evaluării anuale de către entitate a riscurilor operaționale generate de utilizarea sistemelor informatice importante prevăzută la <u>art. 6 alin. (1)</u> din prezenta normă	Opinie cu privire la plauzibilitatea metodologiei/tehnichilor utilizate, precum și asupra măsurilor de control implementate în vederea adresării riscurilor operaționale identificate
N	Rezultatul obținut în urma efectuării testului de penetrare, după caz	În situația efectuării testului de penetrare de către auditorul IT, se va menționa: - descrierea metodologiei/tehnichilor utilizate; - menționarea rezultatelor obținute în urma testului; - recomandările adresate entității și răspunsul managementului entității. În situația în care testul de penetrare nu a fost efectuat de către auditorul IT, acesta va verifica: - metodologia/tehnichile utilizate; - rezultatele obținute în urma testului; - recomandările adresate entității și răspunsul managementului entității.
O	Afirmația 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 observațiilor

Anexa este însoțită de către entitatea auditată prin semnarea acesteia către reprezentantul legal și conține, fără a se limita la acestea:

- descrierea neconformității/constatării;
- importanța neconformității/constatării;
- riscurile asociate;
- probabilitatea ca aceste constatări să aibă un impact semnificativ; recomandările auditorului IT pentru acțiuni corective și răspunsul conducerii entității auditate pentru fiecare constatare din raport (inclusiv în urma testului de penetrare);
- planul de acțiune asumat de către entitatea auditată care conține măsurile efective, termenul de implementare și persoanele responsabile de implementare.

2. Analiza internă a riscurilor operaționale și registrul riscurilor

Anexa conține următoarele informații, fără a se limita la acestea:

- descrierea politicii/metodologiei utilizate de către entitate;
- rezultatele revizuirii riscurilor generate de utilizarea sistemelor informatice;
- rezultatele evaluării de către auditorul IT a măsurilor de control implementate în vederea adresării riscurilor operaționale identificate (pentru riscuri semnificative).

3. Cerințe referitoare la furnizorii externi și furnizorii de servicii IT externalizate pentru sistemele informatice importante

Raportarea se efectuează prin completarea tabelului prezentat

Sistem informatic important	Funcția sistemului informatic important - descrierea serviciilor oferite	Furnizor - date de identificare (denumire, sediul entității, 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/Parțial	Comentarii
-----------------------------	--	--	---	---	--	------------

4. Organizarea pe procese

Anexa cuprinde informații referitoare la managementul disponibilității, respectiv:

- măsurarea disponibilității sistemelor informatice importante (conform cu cerințele standardului TIA-942 tier 2);
- sistemele informatice importante pentru care s-au efectuat măsurătorile cu privire la disponibilitatea acestora;
- descrierea modului în care a fost efectuată măsurarea disponibilității 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 cerințelor impuse

Nr.	Articol supus verificării	Conformitate DA/NU/PARȚIAL/NEAPLICABIL	Comentarii/Motivații în cazul nerespectării prevederilor
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. Declarația pe propria răspundere a auditorului IT extern

Anexa conține informații cu privire la faptul că acesta nu se află în relații cu entitatea auditată, cu membrii structurii de conducere sau cu angajații acesteia care ar putea să îi afecteze independența sau obiectivitatea activității de audit IT.

7. Declarație pe propria răspundere a reprezentantului legal al entității auditate IT cu resurse interne

Anexa conține informații cu privire la efectuarea auditului IT cu resurse interne certificate care sunt independente față de activitatea auditată și 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, entitățile 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 sfârșitul perioadei de raportare;
- c)** valoarea indicatorului - dacă sunt înregistrate valori diferite de zero ale indicatorului respectiv pentru perioada raportată sau, după caz, la sfârșitul perioadei de raportare.

Obiectiv în perioada de raportare	Indicator
1	2
Indicatori referitori la accesarea online a serviciilor oferite de entitate	
	Număr de clienți (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 entității (referitor la portofolii, tranzacții și 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 entității (programe informatice interne/externe/online accesate via internet)
Indicatori referitori la principiul dublei validări prin operațiuni în sistemele informatice importante	
	Număr de operațiuni INIȚIAȚE care presupun dubla validare
	Număr de operațiuni CONFIRMATE care presupun dubla validare
	Număr de operațiuni 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 conțin informații referitoare la portofolii, tranzacții și active
	Număr administratori de sistem (total utilizatori) care au acces la credențialele conturilor de acces ale clienților
Indicatori referitori la incidente interne de securitate informatică, declarate	
	Număr total incidente interne de securitate informatică
	Număr total incidente informatice externe
	Număr încălcări politică și proceduri securitate
	Număr pierderi date generate de acțiuni neaprobat
	Număr incidente declarate aferente pierderii de date (date electronice)
	Număr de incidente declarate care au dus la distrugere accidentală sau intenționată de documente/înregistrări/fișiere
	Număr de incidente declarate de încălcare gravă a regulilor/fraude/înșelătorii
	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 agreeate interne și pentru clienți	
	Număr de ore de indisponibilitate neprogramată a sistemelor informatice importante la care au acces clienții (precum, dar nelimitat la aplicații de tranzacționare online, aplicații online pentru subscrierea de polițe de asigurare)
	Număr de ore de indisponibilitate neprogramată a serviciilor IT externalizate care afectează serviciile oferite către clienții entităților
Management schimbări	
	Numărul programelor informatice importante
	Numărul de modificări aduse programelor informatice importante
	Număr erori în exploatare generate de deficiențe în proiectarea sistemelor informatice importante
	Număr erori în exploatare neidentificate în testarea sistemelor informatice importante
Indicatori managementul continuității	
	Număr de teste efectuate conform planului de continuitate a afacerii
	Număr de teste efectuate conform planului de recuperare în caz de dezastru
Audituri și testări	
	Număr de audituri interne anuale
