MONITORUL OFICIAL AL ROMÂNIEI

Anul 183 (XXVII) — Nr. 227

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Vineri, 3 aprilie 2015

SUMAR

L E G I Ș I D E C R E T E

PARLAMENTUL ROMÂNIEI

C A M E R A D E P U T A Ț I L O R **S E N A T U L**

L E G E
pentru ratificarea Acordului euromediteranean în domeniul aviației între Uniunea Europeană și statele sale membre, pe de o parte, și Guvernul Statului Israel, pe de altă parte, semnat la Luxemburg la 10 iunie 2013

Parlamentul României adoptă prezenta lege.

Articol unic. — Se ratifică Acordul euromediteranean în domeniul aviației între Uniunea Europeană și statele sale membre, pe de o parte, și Guvernul Statului Israel, pe de altă parte, semnat la Luxemburg la 10 iunie 2013*).

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (2) din Constituția României, republicată.

PREȘEDINTELE CAMEREI DEPUTAȚILOR
VALERIU-ȘTEFAN ZGONEA

p. PREȘEDINTELE SENATULUI,
CRISTIAN-SORIN DUMITRESCU

București, 3 martie 2015.
Nr. 19.

*) Acordul euromediteranean în domeniul aviației între Uniunea Europeană și statele sale membre, pe de o parte, și Guvernul Statului Israel, pe de altă parte, semnat la Luxemburg la 10 iunie 2013, se publică în Monitorul Oficial al României, Partea I, nr. 227 bis, care se poate achiziționa de la Centrul pentru relații cu publicul al Regiei Autonome „Monitorul Oficial”, București, șos. Panduri nr. 1.

PREȘEDINTELE ROMÂNIEI

D E C R E T
privind promulgarea Legii pentru ratificarea Acordului euromediteranean în domeniul aviației între Uniunea Europeană și statele sale membre, pe de o parte, și Guvernul Statului Israel, pe de altă parte, semnat la Luxemburg la 10 iunie 2013

În temeiul prevederilor art. 77 alin. (1) și ale art. 100 alin. (1) din Constituția României, republicată,

Președintele României d e c r e t e a z ă:

Articol unic. — Se promulgă Legea pentru ratificarea Acordului euromediteranean în domeniul aviației între Uniunea Europeană și statele sale membre, pe de o parte, și Guvernul Statului Israel, pe de altă parte, semnat la Luxemburg la 10 iunie 2013, și se dispune publicarea acestei legi în Monitorul Oficial al României, Partea I.

PREȘEDINTELE ROMÂNIEI
KLAUS-WERNER IOHANNIS

București, 2 martie 2015.
Nr. 296.

DECIZII ALE CURȚII CONSTITUȚIONALE

CURTEA CONSTITUȚIONALĂ

DECIZIA Nr. 68
din 26 februarie 2015

referitoare la excepția de neconstituționalitate a prevederilor art. 4 teza a doua raportate la cele ale art. 1 alin. (3), art. 24 alin. (2)—(4) și art. 33—35 din Legea nr. 165/2013 privind măsurile pentru finalizarea procesului de restituire, în natură sau prin echivalent, a imobilelor preluate în mod abuziv în perioada regimului comunist în România

Augustin Zegrean	— președinte
Valer Dorneanu	— judecător
Petre Lăzăroiu	— judecător
Mircea Ștefan Minea	— judecător
Daniel Marius Morar	— judecător
Mona-Maria Pivniceru	— judecător
Puskás Valentin Zoltán	— judecător
Simona-Maya Teodoroiu	— judecător
Tudorel Toader	— judecător
Valentina Bărbățeanu	— magistrat-asistent

Cu participarea reprezentantului Ministerului Public, procuror Liviu-Daniel Arcer.

1. Pe rol se află soluționarea excepției de neconstituționalitate a prevederilor art. 1 alin. (3), art. 4, art. 24 și art. 31—35 din Legea nr. 165/2013 privind măsurile pentru finalizarea procesului de restituire, în natură sau prin echivalent, a imobilelor preluate în mod abuziv în perioada regimului comunist în România, excepție ridicată de Adriana-Cristina Aronovici și Societatea Comercială „Real Grup Invest” — S.A. din București în Dosarul nr. 8.957/3/2012 al Tribunalului București — Secția a V-a civilă și care constituie obiectul Dosarului nr. 535D/2014 al Curții Constituționale.

2. La apelul nominal se constată lipsa părților. Procedura de citare este legal îndeplinită.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantului Ministerului Public, care pune concluzii de respingere a excepției de neconstituționalitate a prevederilor art. 4 teza a doua raportate la art. 33 din Legea nr. 165/2013, ca devenită inadmisibilă după pronunțarea Deciziei nr. 88 din 27 februarie 2014. În ce privește prevederile art. 1 alin. (2) și art. 24 din Legea nr. 165/2013 apreciază că nu sunt aplicabile în cauza în care a fost ridicată excepția de neconstituționalitate, astfel că pune concluzii de respingere, ca inadmisibilă, a acesteia. Referitor la dispozițiile art. 31—35 din Legea nr. 165/2013 consideră că nu contravin prevederilor constituționale invocate.

C U R T E A,

având în vedere actele și lucrările dosarului, constată următoarele:

4. Prin Sentința civilă din 9 iulie 2013, pronunțată în Dosarul nr. 8.957/3/2012, **Tribunalul București — Secția a V-a civilă a sesizat Curtea Constituțională cu excepția de neconstituționalitate a prevederilor art. 1 alin. (3), art. 4, art. 24 și art. 31—35 din Legea nr. 165/2013 privind măsurile pentru finalizarea procesului de restituire, în natură sau prin echivalent, a imobilelor preluate în mod abuziv în perioada regimului comunist în România**, excepție ridicată de Adriana-Cristina Aronovici și Societatea Comercială „Real Grup Invest” — S.A. din București —, aceasta din urmă în calitate de cesionar al unui procent din dreptul la măsuri reparatorii în echivalent cuvenit persoanei îndreptățite Adriana-Cristina Aronovici —, într-o cauză civilă având ca obiect soluționarea de către instanță, în conformitate cu Legea nr. 10/2001, a notificării referitoare la restituirea în natură a unui teren și la acordarea de măsuri reparatorii în echivalent pentru o construcție, notificare pe care primarul municipiului București a refuzat în mod nejustificat să o soluționeze.

5. **În motivarea excepției de neconstituționalitate**, autorii acesteia susțin, în esență, că, prin raportare la art. 4 din Legea nr. 165/2013, prevederile art. 33 din aceeași lege încalcă principiul neretroactivității legii în ipoteza în care termenele stabilite prin acestea se aplică și proceselor aflate în curs de judecată, începute înainte de intrarea în vigoare a Legii nr. 165/2013. Arată, totodată, că prevederile art. 4 și art. 33—35 din Legea nr. 165/2013 creează inegalități între persoanele care au depus cereri, potrivit Legii nr. 10/2001, la entitățile învestite de lege aflate în diverse localități din țară, prin termenele diferite de soluționare pe care le stabilesc și, în același timp, aduc atingere dreptului de acces liber la justiție, exercitarea acestuia fiind interzisă în perioadele pe care Legea nr. 165/2013 le fixează.

6. În ceea ce privește prevederile art. 1 alin. (3) din Legea nr. 165/2013, potrivit cărora în cazul în care titularul a înstrăinat drepturile ce i se cuvin în temeiul legilor de despăgubire singura măsură reparatorie care se acordă este compensarea prin puncte, se susține că încalcă principiul neretroactivității legii, deoarece acestea își extind efectul asupra raporturilor juridice particulare încheiate potrivit legii care avea la bază principiul reparării integrale și cel al restituirii în natură. Se nesocotește, astfel, și principiul egalității, tratând în mod diferit titularii drepturilor exercitate în perioada permisă de legile speciale de reparație cărora autoritățile nu le-au respectat dreptul de petiționare, față de cei care și-au înstrăinat dreptul, cu lipsirea acestora de șansa restituirii în natură a imobilului uzurpat și de beneficiul reparației integrale, existent în momentul formulării cererii. Mai arată că dobânditorii drepturilor, care au avut neșansa de a fi surprinși de apariția noii legi, nu mai pot beneficia de aceleași măsuri reparatorii bazate pe principiul restituirii în natură de care ar fi trebuit să beneficieze autorii lor în lipsa încheierii actelor de înstrăinare.

7. Autorii excepției mai susțin că dreptul de proprietate privată este grav afectat de prevederile art. 24 alin. (2) din Legea nr. 165/2013, care nesocotesc libertatea de a dispune de dreptul de proprietate, limitându-l la 15% din dreptul de proprietate, ceea ce echivalează cu o expropriere lipsită de o cauză de utilitate publică, fără o dreaptă și prealabilă despăgubire, dar și

cu o confiscare a averii dobândită în condiții de perfectă legalitate.

8. **Tribunalul București — Secția a V-a civilă** consideră că dispozițiile art. 4 din Legea nr. 165/2013 sunt neconstituționale în măsura în care termenele prevăzute la art. 33 din aceeași lege se aplică și cauzelor aflate pe rolul instanțelor la data intrării în vigoare a legii. În ce privește celelalte prevederi de lege criticate apreciază că sunt constituționale.

9. Potrivit prevederilor art. 30 alin. (1) din Legea nr. 47/1992, actul de sesizare a fost comunicat președinților celor două Camere ale Parlamentului, Guvernului și Avocatului Poporului, pentru a-și exprima punctele de vedere asupra excepției de neconstituționalitate.

10. **Avocatul Poporului** precizează că, urmare a deciziilor Curții Constituționale nr. 88 din 27 februarie 2014 și nr. 269 din 7 mai 2014, excepția de neconstituționalitate a prevederilor art. 4 teza a doua raportate la art. 33 și 34 din Legea nr. 165/2013 a devenit inadmisibilă. Referitor la celelalte prevederi de lege criticate apreciază că sunt constituționale.

11. **Președinții celor două Camere ale Parlamentului** și **Guvernul** nu au comunicat punctele lor de vedere asupra excepției de neconstituționalitate.

C U R T E A,

examinând actul de sesizare, punctul de vedere al Avocatului Poporului, raportul întocmit de judecătorul-raportor, concluziile procurorului, dispozițiile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

12. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art. 146 lit. d) din Constituție, precum și ale art. 1 alin. (2), ale art. 2, 3, 10 și 29 din Legea nr. 47/1992, să soluționeze excepția de neconstituționalitate.

13. Obiectul excepției de neconstituționalitate îl constituie, potrivit actului de sesizare, prevederile art. 1 alin. (3), art. 4, art. 24 și art. 31—35 din Legea nr. 165/2013 privind măsurile pentru finalizarea procesului de restituire, în natură sau prin echivalent, a imobilelor preluate în mod abuziv în perioada regimului comunist în România, publicată în Monitorul Oficial al României, Partea I, nr. 278 din 17 mai 2013. Din motivarea scrisă a excepției de neconstituționalitate, Curtea observă, însă, că autorii acesteia critică doar prevederile art. 4 teza a doua raportate la cele ale art. 1 alin. (3), art. 24 alin. (2)—(4) și art. 33—35 din Legea nr. 165/2013, care au următorul conținut:

— Art. 1 alin. (3): *„În situația în care titularul a înstrăinat drepturile care i se cuvin potrivit legilor de restituire a proprietății, singura măsură reparatorie care se acordă este compensarea prin puncte potrivit art. 24 alin. (2), (3) și (4).”;*

— Art. 4 teza a doua: *„Dispozițiile prezentei legi se aplică (...) cauzelor în materia restituirii imobilelor preluate abuziv, aflate pe rolul instanțelor, (...) la data intrării în vigoare a prezentei legi.”;*

— Art. 24 alin. (2)—(4): *„(2) În dosarele în care se acordă măsuri compensatorii altor persoane decât titularul dreptului de proprietate, fost proprietar sau moștenitorii legali ori testamentari ai acestuia, se acordă un număr de puncte egal cu suma dintre prețul plătit fostului proprietar sau moștenitorilor legali ori testamentari ai acestuia pentru tranzacționarea dreptului de proprietate și un procent de 15% din diferența până la valoarea imobilului stabilită conform art. 21 alin. (6).*

(3) Numărul de puncte acordat în condițiile alin. (2) nu poate reprezenta o valoare mai mare decât cea stabilită potrivit art. 21 alin. (6) și (7).

(4) În cazul în care din documentele depuse la dosarul de restituire nu rezultă prețul plătit fostului proprietar sau moștenitorilor legali ori testamentari ai acestuia pentru tranzacționarea dreptului de proprietate, punctele vor reprezenta echivalentul a 15% din valoarea stabilită conform art. 21 alin. (6).”;

— Art. 33: *„(1) Entitățile învestite de lege au obligația de a soluționa cererile formulate potrivit Legii nr. 10/2001, republicată, cu modificările și completările ulterioare, înregistrate și nesoluționate până la data intrării în vigoare a prezentei legi și de a emite decizie de admitere sau de respingere a acestora, după cum urmează:*

a) în termen de 12 luni, entitățile învestite de lege care mai au de soluționat un număr de până la 2.500 de cereri;

b) în termen de 24 de luni, entitățile învestite de lege care mai au de soluționat un număr cuprins între 2.500 și 5.000 de cereri;

c) în termen de 36 de luni, entitățile învestite de lege care mai au de soluționat un număr de peste 5.000 de cereri.

(2) Termenele prevăzute la alin. (1) curg de la data de 1 ianuarie 2014.

(3) Entitățile învestite de lege au obligația de a stabili numărul cererilor înregistrate și nesoluționate, de a afișa aceste date la sediul lor și de a le comunica Autorității Naționale pentru Restituirea Proprietăților. Datele transmise de entitățile învestite de lege vor fi centralizate și publicate pe pagina de internet a Autorității Naționale pentru Restituirea Proprietăților.

(4) Cererile se analizează în ordinea înregistrării lor la entitățile prevăzute la alin. (1).”;

— Art. 34: *„(1) Dosarele înregistrate la Secretariatul Comisiei Centrale pentru Stabilirea Despăgubirilor vor fi soluționate în termen de 60 de luni de la data intrării în vigoare a prezentei legi, cu excepția dosarelor de fond funciar, care vor fi soluționate în termen de 36 de luni.*

(2) Dosarele care vor fi transmise Secretariatului Comisiei Naționale ulterior datei intrării în vigoare a prezentei legi vor fi soluționate în termen de 60 de luni de la data înregistrării lor, cu excepția dosarelor de fond funciar, care vor fi soluționate în termen de 36 de luni.

(3) Numărul dosarelor prevăzute la alin. (1) și data înregistrării dosarelor prevăzute la alin. (2) se publică pe pagina de internet a Autorității Naționale pentru Restituirea Proprietăților și se comunică, la cerere, persoanelor îndreptățite.”;

— Art. 35: *„(1) Deciziile emise cu respectarea prevederilor art. 33 și 34 pot fi atacate de persoana care se consideră îndreptățită la secția civilă a tribunalului în a cărui circumscripție se află sediul entității, în termen de 30 de zile de la data comunicării.*

(2) În cazul în care entitatea învestită de lege nu emite decizia în termenele prevăzute la art. 33 și 34, persoana care se consideră îndreptățită se poate adresa instanței judecătorești prevăzute la alin. (1) în termen de 6 luni de la expirarea termenelor prevăzute de lege pentru soluționarea cererilor.

(3) În cazurile prevăzute la alin. (1) și (2), instanța judecătorească se pronunță asupra existenței și întinderii dreptului de proprietate și dispune restituirea în natură sau, după caz, acordarea de măsuri reparatorii în condițiile prezentei legi.

(4) Hotărârile judecătorești pronunțate potrivit alin. (3) sunt supuse numai apelului.

(5) Cererile sau acțiunile în justiție formulate în temeiul alin. (1) și (2) sunt scutite de taxa judiciară de timbru.”

14. În opinia autorilor excepției, textele de lege criticate contravin următoarelor prevederi din Constituție: art. 1 alin. (5)

care impune obligația respectării Constituției, a supremației sale și a legilor, art. 15 alin. (2) care instituie principiul neretroactivității legii, art. 16 alin. (1) și (2) care consacră principiul egalității în fața legii și a autorităților publice, art. 21 alin. (1)—(3) referitor la dreptul de acces liber la justiție și la un proces echitabil, soluționat într-un termen rezonabil, art. 44 care garantează dreptul de proprietate privată și creanțele asupra statului și care instituie egalitatea în ceea ce privește garantarea și ocrotirea prin lege a acestui drept și art. 53 care stabilește condițiile în care este permisă restrângerea exercițiului unor drepturi sau al unor libertăți. Se invocă, de asemenea, art. 6 paragraful 1 care statuează cu privire la dreptul la un proces echitabil și art. 14 privind interzicerea discriminării din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, precum și art. 1 — *Protecția proprietății* din Primul Protocol adițional la aceeași convenție.

15. Examinând excepția de neconstituționalitate, Curtea reține, în ce privește excepția de neconstituționalitate a dispozițiilor art. 4 teza a doua raportate la art. 33—35 din Legea nr. 165/2013, că procesul în cadrul căruia a fost ridicată prezenta excepție de neconstituționalitate are ca obiect soluționarea cererii adresate instanței de o persoană care se consideră îndreptățită la obținerea de măsuri reparatorii și de cesionarul unui procent din dreptul la despăgubiri al acesteia, pentru ca instanța, în conformitate cu Legea nr. 10/2001 privind regimul juridic al unor imobile preluate în mod abuziv în perioada 6 martie 1945—22 decembrie 1989, să soluționeze notificarea referitoare la restituirea în natură a unui teren și la acordarea de măsuri reparatorii în echivalent pentru o construcție demolată, notificare pe care primarul municipiului București nu a soluționat-o în termenul de 60 de zile prevăzut de art. 25 din Legea nr. 10/2001.

16. Față de acest cadru procesual, Curtea constată că dispozițiile art. 4 teza a doua raportate la cele ale art. 34 și 35 din Legea nr. 165/2013 nu au legătură cu soluționarea cauzei aflate pe rolul instanței care a sesizat Curtea Constituțională. Astfel, art. 34 din Legea nr. 165/2013, referitor la soluționarea dosarelor de către Comisia Centrală pentru Stabilirea Despăgubirilor, vizează o etapă procesuală ulterioară în desfășurarea demersurilor legale întreprinse în vederea recunoașterii și valorificării dreptului la măsuri reparatorii pentru imobilul preluat abuziv în timpul regimului comunist. Tot astfel, art. 35 din Legea nr. 165/2013 are în vedere o cale de atac ce poate fi introdusă împotriva deciziilor emise potrivit art. 33 și 34 din aceeași lege, așadar un text de lege care, teoretic, va fi aplicabil abia după scurgerea termenelor prevăzute de cele două articole menționate.

17. Ca atare, cele două texte de lege criticate nu sunt aplicabile în această etapă a procedurii de restituire a imobilelor la care se referă Legea nr. 165/2013, ceea ce determină, în temeiul art. 29 alin. (1) din Legea nr. 47/1992, respingerea, ca inadmisibilă, a excepției de neconstituționalitate privind dispozițiile art. 4 teza a doua raportate la cele ale art. 34 și 35 din Legea nr. 165/2013.

18. În ceea ce privește prevederile art. 4 teza a doua raportate la cele ale art. 33 din Legea nr. 165/2013, prin Decizia nr. 88 din 27 februarie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 281 din 16 aprilie 2014, Curtea a constatat că prevederile art. 4 teza a doua din Legea nr. 165/2013 sunt constituționale în măsura în care termenele prevăzute la art. 33 din aceeași lege nu se aplică și cauzelor în materia restituirii imobilelor preluate abuziv, aflate pe rolul instanțelor la data intrării în vigoare a legii.

19. Întrucât autorii excepției de față critică aceeași interpretare care a fost constatată ca neconstituțională prin decizia menționată și având în vedere că această decizie a fost pronunțată ulterior sesizării instanței constituționale cu soluționarea prezentei excepții, rezultă că excepția de neconstituționalitate a dispozițiilor art. 4 teza a doua raportate la art. 33 din Legea nr. 165/2013 a devenit inadmisibilă.

20. Curtea reamintește, totodată, că, în virtutea prevederilor art. 147 alin. (1) și (4) din Constituție, instanța de judecată și instituțiile abilitate să aplice legea în cauză vor respecta deciziile Curții Constituționale în procesul de aplicare și interpretare a legislației incidente în speța dedusă soluționării, atât sub aspectul dispozitivului, cât și al considerentelor pe care acesta se sprijină. De aceea, chiar dacă excepția de neconstituționalitate a dispozițiilor art. 4 teza a doua raportat la art. 33 din Legea nr. 165/2013 urmează să fie respinsă ca devenită inadmisibilă, în temeiul art. 29 alin. (3) din Legea nr. 47/1992, decizia anterioară de constatare a neconstituționalității acestora reprezintă temei al revizuirii conform art. 322 pct. 10 din Codul de procedură civilă din 1865 sau art. 509 pct. 11 din Codul de procedură civilă, după caz, în cauza în care a fost invocată prezenta excepție (a se vedea, în acest sens, Decizia nr. 122 din 6 martie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 389 din 27 mai 2014).

21. Cu privire la excepția de neconstituționalitate a dispozițiilor art. 4 teza a doua raportate la art. 1 alin. (3) și art. 24 alin. (2)—(4) din Legea nr. 165/2013, Curtea observă că, prin Decizia nr. 200 din 3 aprilie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 448 din 19 iunie 2014, a examinat textele de lege menționate din perspectiva unor critici similare celor formulate în prezenta cauză și a reținut că acestea sunt în concordanță cu prevederile constituționale și convenționale invocate și de autorii excepției de față.

22. Cu acel prilej, Curtea a observat că prevederile art. 1 alin. (3) din Legea nr. 165/2013 stabilesc că cesionarului i se acordă, ca unică măsură reparatorie, compensarea prin puncte, numărul de puncte de care acesta va putea beneficia fiind, potrivit art. 24 alin. (2) din Legea nr. 165/2013, egal cu suma dintre prețul plătit fostului proprietar sau moștenitorilor legali ori testamentari ai acestuia pentru tranzacționarea dreptului de proprietate, la care se adaugă și un procent de 15% din diferența până la valoarea imobilului, astfel cum aceasta rezultă din grila notarială valabilă la data intrării în vigoare a legii.

23. Analizând art. 1 alin. (3) și art. 24 alin. (2)—(4) din Legea nr. 165/2013, Curtea a reținut că legiuitorul a reglementat în mod diferit modalitatea de despăgubire, în raport cu persoana beneficiarilor măsurilor reparatorii conferite de Legea nr. 165/2013, și anume titularul dreptului la măsuri reparatorii în temeiul legislației reparatorii anterioare, pe de o parte, și persoanele către care au fost înstrăinate drepturile cuvenite potrivit legilor de restituire a proprietății, pe de altă parte. Curtea a statuat că această opțiune a legiuitorului nu reprezintă o sancționare a titularilor originari ai acestui drept care au înstrăinat dreptul la obținerea măsurilor reparatorii, dat fiind faptul că, prin ipoteză, în patrimoniul acestora nu se mai regăsește acest drept. Ca efect al cesiunii de creanță specifice, încheiată anterior intrării în vigoare a noii legi reparatorii, dreptul pretins de cedenți — constând în acordarea măsurilor reparatorii conferite de legislația anterioară în domeniul proprietăților preluate în mod abuziv — a fost transferat către cesionari.

24. În ceea ce privește pretinsa discriminare creată prin textele de lege criticate, Curtea a reținut că acordarea unor măsuri reparatorii diferite, în funcție de beneficiarii acestora, echivalează cu instituirea unui tratament juridic diferit, dar care

nu constituie, însă, o discriminare, întrucât, în sensul jurisprudenței Curții Constituționale, nu orice diferență de tratament semnifică, în mod automat, încălcarea dispozițiilor art. 16 alin. (1) din Constituție sau a celor convenționale referitoare la interzicerea discriminării. Astfel, față de obiectul de reglementare al Legii nr. 165/2013, opțiunea legiuitorului de a exclude de la măsura reparatorie a restituirii în natură, precum și de la cea a compensării integrale prin puncte a persoanelor în patrimoniul cărora a fost transmis, prin intermediul unor contracte cu titlu oneros, dreptul de a obține măsurile reparatorii apare ca fiind justificată în mod obiectiv și rezonabil, având în vedere că asupra acestora din urmă nu s-au răsfrânt direct sau indirect măsurile de preluare abuzivă. Aceasta, deoarece legislația cu caracter reparator a vizat exclusiv titularul dreptului sau moștenitorii acestuia.

25. Mai mult, întrucât legiuitorul a acordat cesionarilor dreptului la despăgubire un număr de puncte egal cu suma dintre prețul plătit pentru tranzacționarea dreptului de proprietate și un procent de 15% din diferența până la valoarea imobilului, Curtea a reținut că măsura legislativă criticată păstrează un raport rezonabil de proporționalitate între scopul urmărit — despăgubirea integrală doar a titularilor originari ai măsurilor reparatorii sau a moștenitorilor acestora — și mijloacele folosite, cesionarul urmând a obține atât prețul plătit fostului proprietar sau moștenitorilor legali ori testamentari ai acestuia, cât și un procent de 15% din diferența până la valoarea imobilului.

26. Cu privire la invocarea încălcării dispozițiilor art. 15 alin. (2) din Constituție, Curtea a observat, prin Decizia nr. 328 din 12 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 540 din 21 iulie 2014, că, astfel cum rezultă din dispozițiile art. 41 alin. (1) din Legea nr. 165/2013, prevederile legale criticate referitoare la plafonarea despăgubirilor acordate cesionarilor nu se aplică celor cărora li s-a stabilit dreptul de proprietate și li s-a emis titlul de despăgubire anterior intrării în vigoare a Legii nr. 165/2013. Prin urmare, prevederile de lege criticate nu se aplică retroactiv, ci reglementează modul de acțiune în timpul următor intrării în vigoare a legii, adică în domeniul ei propriu de aplicare.

27. Totodată, prin Decizia nr. 321 din 10 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 583 din 8 august 2014, Curtea a remarcat că diferența de tratament între cesionarii de drepturi ale căror cereri de chemare în judecată s-au soluționat anterior intrării în vigoare a Legii nr. 165/2013 față de cei care nu au obținut o atare hotărâre derivă din succesiunea în timp a actelor normative în materie. Din această perspectivă, deosebirea de tratament juridic este întemeiată pe un criteriu obiectiv și rezonabil. În legătură cu acest aspect, Curtea a mai reținut că situația diferită în care se află cetățenii în funcție de reglementarea aplicabilă potrivit principiului *tempus regit actum* nu poate fi privită ca o încălcare a dispozițiilor constituționale care consacră egalitatea în fața legii și a autorităților publice, fără privilegii și discriminări. Curtea a constatat că respectarea egalității în drepturi presupune luarea în considerare a tratamentului pe care legea îl prevede față de cei cărora li se aplică în decursul perioadei în care reglementările sale sunt în vigoare, iar nu în raport cu efectele produse prin reglementările legale anterioare. În consecință, reglementările juridice succesive pot prezenta în mod firesc diferențe determinate de condițiile obiective în care ele au fost adoptate. Mai mult, Curtea reține că, în privința obiectului de reglementare a legii analizate, intervenția legiuitorului nu este una aleatorie, ci a fost justificată și impusă firesc ca urmare a pronunțării Hotărârii-pilot din 12 octombrie 2010, pronunțată de Curtea Europeană a Drepturilor Omului în Cauza *Maria Atanasiu și alții împotriva României.*

28. Pentru considerentele expuse mai sus, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, precum și al art. 1—3, al art. 11 alin. (1) lit. A.d) și al art. 29 din Legea nr. 47/1992, cu unanimitate de voturi,

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

I. Respinge, ca inadmisibilă, excepția de neconstituționalitate a prevederilor art. 4 teza a doua raportate la cele ale art. 34 și art. 35 din Legea nr. 165/2013 privind măsurile pentru finalizarea procesului de restituire, în natură sau prin echivalent, a imobilelor preluate în mod abuziv în perioada regimului comunist în România, excepție ridicată de Adriana-Cristina Aronovici și Societatea Comercială „Real Grup Invest” — S.A. din București în Dosarul nr. 8.957/3/2012 al Tribunalului București — Secția a V-a civilă.

II. Respinge, ca devenită inadmisibilă, excepția de neconstituționalitate a prevederilor art. 4 teza a doua raportate la cele ale art. 33 din Legea nr. 165/2013, excepție ridicată de aceiași autori în același dosar al aceleiași instanțe.

III. Respinge, ca neîntemeiată, excepția de neconstituționalitate ridicată de aceiași autori în același dosar al aceleiași instanțe și constată că dispozițiile art. 4 teza a doua raportate la cele ale art. 1 alin. (3) și art. 24 alin. (2)—(4) din Legea nr. 165/2013 sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Tribunalului București — Secția a V-a civilă și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 26 februarie 2015.

PREȘEDINTELE CURȚII CONSTITUȚIONALE
AUGUSTIN ZEGREAN

Magistrat-asistent,
Valentina Bărbățeanu

ACTE ALE AUTORITĂȚII DE SUPRAVEGHERE FINANCIARĂ

AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

NORMĂ
privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile reglementate, autorizate/avizate și/sau supravegheate de Autoritatea de Supraveghere Financiară

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 18 martie 2015,

Autoritatea de Supraveghere Financiară emite următoarea normă:

CAPITOLUL I
Dispoziții generale

Art. 1. — (1) Prezenta normă stabilește cerințele la nivelul entităților autorizate/avizate, 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 de fapte ce țin de criminalitatea informatică.

(2) Prezenta normă stabilește activități și operațiuni pentru evaluarea, supravegherea și controlul riscurilor operaționale generate de utilizarea sistemelor informatice și ale securității informatice.

Art. 2. — Prezenta normă se aplică următoarelor categorii de entități autorizate/avizate, reglementate și/sau supravegheate de A.S.F., denumite în continuare *entități*:

a) operatori de piață/operatori de sistem;

b) societăți de administrare a investițiilor (SAI), organisme de plasament colectiv (OPC și AOPC) care se autoadministrează, după cum urmează:

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

2. societăți cu 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.) încadrate la art. 6 alin. (1) din Legea nr. 297/2004 privind piața de capital, cu modificările și completările ulterioare, sucursale ale intermediarilor din state nemembre și instituții de credit din România autorizate de Banca Națională a României în conformitate cu legislația bancară și înscrise în Registrul public al A.S.F. în calitate de intermediar, și anume:

1. intermediari care au calitatea de operator independent;

2. intermediari care prestează servicii conexe, prevăzute la art. 5 alin. (1[1]) lit. a) din Legea nr. 297/2004, cu modificările și completările ulterioare;

3. intermediari care folosesc facilități de tranzacționare prin internet (ADP/AS) — platforme de preluare și transmitere a ordinelor clienților;

4. intermediari care au calitatea de market makeri și/sau furnizori de lichiditate;

5. intermediari care tranzacționează pe cont propriu și nu se încadrează în categoriile de la pct. 1—4;

6. intermediari care nu tranzacționează pe cont propriu și nu se încadrează în categoriile de la pct. 1—4;

e) traderi;

f) Fondul de compensare a investitorilor;

g) societăți de asigurare/reasigurare;

h) brokeri de asigurare/reasigurare;

i) entități care desfășoară activitatea de depozitare a activelor organismelor de plasament colectiv și a fondurilor de pensii private;

j) societăți de administrare a fondurilor de pensii private.

Art. 3. — Termenii și expresiile utilizate în prezenta normă au înțelesul prevăzut în anexa nr. 1.

Art. 4. — (1) Prevederile prezentei norme se aplică de către entități în funcție de categoria de risc stabilită de A.S.F. conform art. 6 alin. (1) și, respectiv, 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, respectiv de impactul asupra activității, în conformitate cu prevederile art. 6 alin. (1).

(3) Entitățile vor participa la colectarea, analizarea, monitorizarea și raportarea evenimentelor de securitate informatică, în cadrul sistemului dezvoltat de A.S.F.

Art. 5. — (1) Entitățile evaluează anual și monitorizează continuu riscurile operaționale generate de utilizarea sistemelor informatice, prioritizează resursele, implementează măsuri de securitate informatică și monitorizează eficacitatea acestora prin aplicarea managementului de risc.

(2) Modalitatea de implementare a măsurilor de securitate informatică este stabilită de fiecare entitate, în funcție de profilul de risc, de riscurile identificate, de incidentele apărute, în conformitate cu cerințele legale aplicabile.

CAPITOLUL II
Încadrarea entităților în categorii de risc

Art. 6. — (1) În scopul prezentei norme, entitățile prevăzute la art. 2 se includ în patru categorii de risc: „risc major”, „risc important”, „risc mediu”, „risc scăzut”, după cum urmează:

a) entitățile prevăzute la art. 2 lit. a), c) și lit. d) pct. 1 reprezintă entități încadrate în categoria de „risc major”;

b) entitățile prevăzute la art. 2. lit. d) pct. 2, 3 și 4, lit. g) și i) reprezintă entități încadrate în categoria de „risc important”;

c) entitățile prevăzute la art. 2 lit. b) pct. 1, lit. d) pct. 5 și lit. f) reprezintă entități încadrate în categoria de „risc mediu”;

d) entitățile prevăzute la art. 2 lit. b) pct. 2, lit. d) pct. 6, lit. e) și h) reprezintă entități încadrate în categoria de „risc scăzut”.

(2) Entitatea care prestează mai multe tipuri de activități autorizate de către A.S.F., încadrându-se astfel în mai multe categorii de risc dintre cele menționate la alin. (1), va respecta obligațiile instituite pentru fiecare activitate autorizată în parte.

(3) Societățile de administrare a fondurilor de pensii private vor fi încadrate individual în categorii de risc, conform prevederilor art. 44 alin. (4) lit. e) și ale art. 51 din Norma Consiliului Autorității de Supraveghere Financiară nr. 3/2014

privind controlul intern, auditul intern și administrarea riscurilor în sistemul de pensii private.

(4) Încadrarea, respectiv reîncadrarea entităților menționate la art. 2 lit. b) se realizează la începutul fiecărui an, în baza valorii totale a activelor în portofoliu/administrate din ultima zi lucrătoare a anului anterior.

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

CAPITOLUL III
Activitățile desfășurate de entități

Art. 7. — (1) Entitățile desfășoară cel puțin activitățile obligatorii corespunzătoare fiecărei categorii de risc prevăzute la art. 6 alin. (1), conform tabelului din anexa nr. 2.

(2) În termen 90 de zile de la publicarea prezentei norme în Monitorul Oficial al României, Partea I, A.S.F. va elabora și publica pe site-ul propriu ghidul de îndrumare care cuprinde detalii și parametrii referitori la modalitatea de implementare a activităților obligatorii menționate la alin. (1). Acest ghid are un caracter orientativ și poate fi actualizat de A.S.F. în funcție de bunele practici în materie.

Art. 8. – (1) Raportat la activitatea desfășurată entitățile se asigură că sistemele informatice utilizate îndeplinesc cel puțin următoarele cerințe:

a) asigură integritatea, confidențialitatea, autenticitatea, disponibilitatea datelor în concordanță cu categoria de risc a sistemului informatic 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 corespunzătoare entităților, așa cum sunt prevăzute în legislația specifică, precum și alte raportări solicitate prin reglementările A.S.F.;

c) asigură reconstituirea rapoartelor și informațiilor supuse verificării;

d) asigură stocarea și păstrarea datelor înregistrate și jurnalizate de către sistemele de tranzacționare și back-office pentru o perioadă de timp în conformitate cu legislația aplicabilă în vigoare. Sistemul de păstrare a datelor trebuie să asigure posibilitatea ca aceste date să poată fi transmise sau puse la dispoziția A.S.F. la cerere;

e) asigură posibilitatea de restaurare a datelor arhivate pe suport digital extern, precum, dar fără a se limita la, informații, date introduse, situații financiare sau alte documente;

f) asigură elemente de identificare a datelor supuse prelucrării sau verificării. Sistemele informatice asigură identificarea exactă a timpului la care au fost efectuate înregistrările și identificarea utilizatorilor sistemului la acel moment;

g) 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;

h) asigură mecanisme de securitate și control al sistemelor informatice, pentru păstrarea în siguranță a datelor și informațiilor stocate, a fișierelor și bazelor de date, inclusiv în situația unor evenimente de risc.

(2) Sistemele informatice care oferă intermediarilor și clienților lor accesul la platforme electronice de tranzacționare, precum și cele care evidențiază operațiuni de compensare, decontare și registru pentru instrumente financiare și operațiuni cu aceste instrumente, asigură cel puțin, fără a se limita la:

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 sisteme;

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;

d) mecanisme de nerepudiere a integrității înregistrării operațiunilor de sistem informatic.

CAPITOLUL IV
Auditarea și testarea sistemului informatic

SECȚIUNEA 1
Auditul informatic

Art. 9. — (1) Entitățile încadrate la categoria de risc major au obligația de a audita extern sistemul informatic utilizat, cu periodicitate anuală.

(2) Entitățile încadrate la categoria de risc important au obligația de a audita, extern sau cu resurse interne certificate, sistemul informatic utilizat, o dată la 2 ani.

(3) Entitățile încadrate la categoria de risc mediu au obligația de a audita, extern sau cu resurse interne certificate, sistemul informatic utilizat, o dată la 3 ani.

(4) Entitățile încadrate la categoria de risc scăzut au obligația de a audita, extern sau cu resurse interne certificate, sistemul informatic utilizat, o dată la 4 ani.

(5) A.S.F. este îndreptățită să instituie în sarcina entității obligația auditării externe a sistemului informatic pentru activitățile solicitate de către A.S.F. dacă:

a) în urma constatărilor rezultă că o entitate nu a desfășurat toate activitățile minime obligatorii categoriei de risc în care aceasta se încadrează, conform prevederilor art. 7, sau activitățile desfășurate au un caracter formal;

b) A.S.F. apreciază că se impune efectuarea unor investigații suplimentare ale sistemelor informatice.

(6) Instituirea de către A.S.F. a obligației de auditare a sistemului IT conform alin. (5) este însoțită de 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 lucrătoare.

(7) Auditul extern se efectuează în baza unui contract încheiat între entitatea care a solicitat auditarea și unul dintre auditorii IT avizați de A.S.F. conform prevederilor art. 10 alin. (2). Entitățile nu pot contracta auditul IT cu același auditor IT pentru mai mult de 3 auditări obligatorii consecutive dintre cele prevăzute la alin. (1)—(4).

(8) Contractul de audit IT prevăzut la alin. (7) cuprinde în mod obligatoriu clauze cu privire la faptul că auditorul IT are obligația de a respecta cerințele necesare efectuării auditului sistemului informatic, în conformitate cu prevederile prezentei norme și cu bunele practici în domeniu.

(9) Contractul menționat la alin. (7) trebuie să conțină o clauză expresă prin care auditorul se obligă să notifice în cel

mai scurt timp posibil și în scris A.S.F. cu privire la orice fapt sau act în legătură cu sistemul informatic și de comunicații utilizat de entitate 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 profesionale sau la o opinie negativă.

(10) Contractul prevăzut la alin. (7) trebuie să conțină o clauză expresă prin care, la solicitarea scrisă a A.S.F., auditorul se obligă să prezinte A.S.F.:

a) orice raport sau document ce a fost adus la cunoștința entității auditate;

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

c) orice alte informații sau documente solicitate în legătură cu activitatea de audit IT la care s-a angajat conform contractului.

(11) Respectarea prevederilor alin. (9) și (10) nu contravine dispozițiilor Codului privind conduita etică și profesională în domeniul auditului financiar, nu constituie o încălcare a niciunei restricții privind divulgarea de informații și nu va atrage niciun fel de răspundere asupra persoanei în cauză. Clauza de confidențialitate nu este opozabilă A.S.F.

Art. 10. — (1) Auditorul IT extern, care intenționează să presteze servicii pentru entitățile cărora le sunt incidente prevederile prezentei norme, are obligația obținerii avizului A.S.F.

(2) În vederea obținerea avizului A.S.F., auditorul IT extern depune la A.S.F. o cerere împreună cu documentația care trebuie să cuprindă următoarele, după caz:

a) datele de identificare ale auditorului:

(i) numele complet/denumirea și adresa/sediul (adresa completă — stradă, număr, bloc, scară, etaj, apartament, oraș, județ/sector, cod poștal);

(ii) datele înregistrării fiscale;

(iii) adresa unde își desfășoară activitatea;

(iv) telefon/fax, e-mail, adresa paginii de internet;

(v) dovada experienței și a specializării pe domeniul de audit al sistemelor informatice;

b) numele și prenumele auditorului persoană fizică certificată și a reprezentantului societății, care vor semna raportul de audit, împreună cu următoarele documente:

(i) copia actului de identitate a auditorului;

(ii) curriculum vitae al auditorului, datat și semnat, cu prezentarea experienței profesionale;

(iii) copia certificatului de auditor IT, semnată pentru conformitate cu originalul;

(iv) certificatul de cazier judiciar și certificatul de cazier fiscal, în original, aflate în termenul de valabilitate;

c) copia contractului/poliței de asigurare de răspundere civilă profesională a auditorului IT, pentru suma asigurată de minimum 100.000 euro;

d) copia documentului de plată a tarifului de înscriere în Registrul public al A.S.F.

(3) Avizarea și înscrierea auditorului IT în Registrul public al A.S.F. sau refuzul avizării, motivat, se realizează în termen de maximum 30 de zile calendaristice de la primirea dosarului complet al solicitantului. Refuzul motivat se transmite auditorului IT. Orice modificare a documentației prevăzute la alin. (2) trebuie transmisă A.S.F. în termen de maximum 30 de zile calendaristice de la data modificării.

(4) A.S.F. retrage avizul auditorului IT extern în oricare dintre următoarele cazuri:

a) la cerere;

b) în cazul lichidării sau la declanșarea insolvenței;

c) în cazul nerespectării, în mod repetat, a prevederilor alin. (3), teza a III-a;

d) în cazul nerespectării prevederilor art. 9 alin. (9) și (10), precum și în cazul nerespectării obligațiilor stabilite în sarcina sa de prezenta normă;

e) din alte cauze prevăzute de legislația în vigoare.

(5) Pentru toate situațiile menționate la alin (4) lit. c)—e), A.S.F. va transmite auditorului IT extern o notificare prealabilă prin care se aduc la cunoștință faptele pentru care se va proceda la retragerea avizului A.S.F.

(6) Entitățile adoptă toate măsurile necesare pentru evitarea conflictelor de interese ce pot interveni în desfășurarea activității de audit IT.

(7) Activitatea de audit trebuie să fie independentă față de activitatea auditată, pentru a nu fi compromisă obiectivitatea activității de audit. Auditorii trebuie să fie independenți și obiectivi în toate aspectele legate de misiunea de audit.

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

(9) La finalizarea auditului IT, auditorii IT au obligația de a întocmi un raport de audit care să cuprindă cel puțin următoarele elemente:

a) titlul raportului, identificarea și descrierea entității auditate, respectiv beneficiarul raportului;

b) destinatarii raportului și orice restricții privind conținutul și circulația raportului;

c) domeniul auditat, obiectivele activității, perioada auditată;

d) natura, cronologia și gradul de acoperire ale procedurilor de audit efectuate;

e) orice calificare de opinie sau limitare a ariei acoperite de audit;

f) datele de identificare ale membrilor echipei de audit, care cuprind cel puțin numele și prenumele, telefon, fax, e-mail și adresa unde își desfășoară activitatea;

g) semnătura coordonatorului certificat al echipei de audit și semnătura reprezentantului legal al auditorului persoană juridică;

h) locul auditării;

i) data raportului;

j) descrierea ariei auditului, incluzând:

(i) descrierea sistemelor auditate;

(ii) măsurile organizatorice: politicile aplicabile și procedurile implementate;

(iii) identificarea aplicațiilor utilizate și a persoanelor implicate;

(iv) componentele sistemelor informatice utilizate;

(v) un sumar conținând analiza riscurilor aferente activității, a posibilelor deficiențe ale sistemului informatic auditat și a măsurilor de reducere a riscurilor asociate, în baza controalelor generale sau specifice implementate conform prezentei norme;

(vi) referire cu privire la corectitudinea raportărilor efectuate în conformitate cu art. 14 alin. (4) aferente perioadei dintre două activități de auditare IT;

(vii) descrierea modului prin care s-a efectuat atacul etic/testul de penetrare, în cazul entităților care sunt obligate să efectueze teste de penetrare conform tabelului din anexa nr. 2;

k) concluziile detaliate ale echipei de audit privind îndeplinirea cerințelor prevăzute la art. 5, 8, 11, 12 și 13, pentru fiecare cerință, cu mențiunea: DA/NU, precum și motivația, în cazul nerespectării acesteia;

l) afirmația de conformitate, reflectată prin „opinia pozitivă” cu privire la conformarea parțială/totală referitoare la obiectivele auditului, indicând punctele care trebuie îmbunătățite, reflectate

prin „opinia cu rezerve/calificată", sau de neîndeplinire a obiectivelor testate/auditate, reflectată prin „opinia negativă";

m) o anexă la raportul de audit IT, însușită de entitatea auditată prin semnarea acesteia de către un reprezentant legal al entității, conținând:

(i) constatările și concluziile;
(ii) neconformitățile, lipsa controalelor sau controale ineficiente;
(iii) importanța neconformității sau deficienței de control;
(iv) probabilitatea ca aceste constatări să aibă un impact semnificativ și riscuri asociate;
(v) recomandările pentru acțiuni corective și răspunsul conducerii entității auditate pentru fiecare constatare din raport, inclusiv termenul de aplicare;
(vi) rezultatul obținut la atacul etic/testul de penetrare, în cazul entităților care sunt obligate să efectueze teste de penetrare conform tabelului din anexa nr. 2;

n) declarația pe propria răspundere a auditorului IT cu privire la faptul că auditul a fost efectuat în conformitate cu prezenta normă și cu standardele de audit în vigoare la momentul realizării auditului, cu menționarea acestora;

o) declarația pe propria răspundere a auditorului IT extern cu privire la faptul că acesta nu se află în relații cu entitatea auditată sau cu angajații entității care ar putea să îi afecteze independența sau obiectivitatea activității de audit.

SECȚIUNEA a 2-a

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

Art. 11. — (1) Entitățile se asigură că, pentru sistemele informatice importante, furnizorii de servicii IT externalizate, inclusiv prin externalizările în lanț, cu excepția furnizorilor de servicii de comunicații, a celor de hardware și de licențe software, raportat strict pentru activitatea externalizată:

a) respectă aceleași cerințe de auditare ca și cele solicitate entității prin prezenta normă;

b) prezintă, la solicitarea A.S.F., modalitatea prin care sunt îndeplinite cerințele adresate entității prin prezenta normă;

c) permit A.S.F. și auditorului IT să verifice și/sau să auditeze sistemele sale informatice conform prezentei norme.

(2) Orice externalizare se realizează cu respectarea prevederilor legale aplicabile incidente sectorului de activitate.

(3) În situațiile în care nu există alte prevederi legale aplicabile sectorului respectiv de activitate, pentru externalizarea unor servicii IT și în toate cazurile în care sunt utilizate serviciile unor furnizori externi, definiți la pct. 28 din anexa nr. 1, entitatea are obligația de a notifica A.S.F., furnizorul extern sau furnizorul de servicii IT externalizate în termen de 10 zile lucrătoare de la momentul încheierii contractului cu acesta, exclusiv pentru sistemele informatice importante.

(4) Notificarea prevăzută la alin. (3) trebuie să includă următoarele informații și documente anexate, după caz:

a) descrierea serviciilor furnizate/externalizate;

b) datele de identificare ale furnizorului:

(i) sediul societății, respectiv adresa completă — stradă, număr, bloc, scară, etaj, apartament, oraș, județ/sector, cod poștal, după caz;
(ii) datele înregistrării fiscale;
(iii) telefon/fax, e-mail, pagina de internet;

c) certificări în funcție de tipul serviciului sau activității desfășurate:

(i) SR ISO/IEC 27001 sau certificări pentru standarde echivalente;
(ii) pentru furnizarea și dezvoltarea de programe informatice software — certificări aferente;
(iii) pentru furnizarea de servicii externalizate — certificări aferente;
(iv) pentru furnizarea de servicii de găzduire sau externalizare prin intermediul centrelor de date — condiții tehnice conform TIA-942 nivel 2 sau echivalent;
(v) pentru furnizarea de servicii de arhivare electronică prin centre de date — autorizare conform prevederilor legale;
(vi) pentru furnizarea de servicii externalizate de tip cloudcomputing public se prezintă certificate specifice activităților externalizate.

(5) În cazul modificării unor informații sau documente, copia sau originalul documentelor modificate se va depune la A.S.F., în termen de maximum 30 de zile calendaristice de la data modificării.

SECȚIUNEA a 3-a

Cerințe cu privire la testarea sistemelor/programelor informatice importante

Art. 12. — (1) Entitățile au obligația de a identifica toate sistemele/programele informatice utilizate și de a le evidenția într-un registru care trebuie să cuprindă:

a) sistemele/programele informatice importante;

b) modificările sistemelor/programelor informatice importante;

c) detalii referitoare la modificările majore ale sistemelor/programelor informatice importante.

(2) În aplicarea prevederilor alin. (1) lit. c), modificările majore se referă la:

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.

Art. 13. — (1) Entitățile au obligația să testeze sistemele/programele 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 cel puțin următoarele elemente:

a) scopul testării;

b) perioada testării;

c) descrierea programului testat;

d) identificarea aplicațiilor utilizate și a persoanelor implicate;

e) analiza riscurilor implicate de achiziția sau modificarea programului informatic important, a posibilelor vulnerabilități și a măsurilor de reducere a riscurilor asociate prin controale de sistem sau de program informatic;

f) descrierea modului prin care s-au efectuat testele, scenariile de test, eventualele norme sau standarde aplicate și rezultatul testării;

g) concluzia echipei de testare;

h) semnătura membrilor echipei de testare.

(3) Rapoartele de testare IT se păstrează la entitate, cel puțin până la următoarea auditare IT, și sunt puse la dispoziția auditorului IT și A.S.F. la cerere.

CAPITOLUL V

Cerințe de raportare

Art. 14. — (1) Entitățile au obligația raportării evaluării prevăzute la art. 5 alin. (1) și a auditării prevăzute la art. 9, astfel:

a) rezultatul evaluării interne a riscurilor operaționale este transmis A.S.F. anual până la 31 martie a anului curent, pentru anul anterior;

b) raportul de audit IT este transmis A.S.F. până la 30 iunie a anului curent, pentru perioada supusă auditării, corespunzătoare fiecărei categorii de risc prevăzute la art. 6 alin. (1).

(2) Entitățile depun raportul de audit IT împreună cu planul de acțiune din care să rezulte modalitatea de remediere a vulnerabilităților identificate pe parcursul derulării activității de audit IT, dacă este cazul.

(3) Rapoartele privind evaluarea internă a riscurilor operaționale prevăzute la alin. (1) lit. a) și rapoartele de audit IT prevăzute la alin. (1) lit. b) se depun la A.S.F. pe suport hârtie sau în format electronic cu semnătură electronică extinsă.

(4) Entitățile transmit până la data de 31 martie a anului curent, pentru anul anterior, o raportare electronică anuală cu indicatorii menționați în anexa nr. 3, în măsura în care acești indicatori sunt aplicabili și sunt aferenți sistemelor informatice importante.

(5) Pentru situațiile în care datele referitoare la anumiți indicatori nu sunt disponibile în cazul unei anumite entități din cauza tipului acesteia, naturii, dimensiunii sau complexității activităților desfășurate de aceasta, în celula corespunzătoare din raport se va insera acronimul N/A (neaplicabil).

CAPITOLUL VI
Contravenții

Art. 15. — Nerespectarea prevederilor prezentei norme de către entitățile prevăzute la art. 2 constituie contravenție conform prevederilor art. 39 alin. (2) lit. a) din Legea nr. 32/2000 privind activitatea de asigurare și supravegherea asigurărilor, cu modificările și completările ulterioare, respectiv ale art. 272 alin. (1) lit. a) pct. 6, lit. b) pct. 5, lit. c) pct. 4, lit. d) pct. 4, lit. e) pct. 6, lit. f) pct. 3, lit. h) pct. 8, lit. j) pct. 17 și lit. k) pct. 3 din Legea nr. 297/2004, cu modificările și completările ulterioare, în funcție de tipul entității.

CAPITOLUL VII
Dispoziții tranzitorii și finale

Art. 16. — (1) Cerințele prevăzute de prezenta normă sunt puse în aplicare de către entități, începând cu data de 1 ianuarie 2016, cu excepția prevederilor art. 11 referitoare la furnizorii externi și furnizorii de servicii IT externalizate care se aplică începând cu data de 30 septembrie 2016, iar entitățile vor transmite notificările menționate la art. 11 alin. (3) până la 31 decembrie 2016.

(2) Până la data de 30 iunie 2016, toate entitățile vor transmite A.S.F. rezultatul primei evaluări interne a riscurilor operaționale prevăzut la art. 14 alin. (1) lit. a), precum și prima raportare electronică prevăzută la art. 14 alin. (4).

(3) Începând cu data de 1 ianuarie 2017, toate entitățile trebuie să efectueze raportările la termenele prevăzute la art. 14.

(4) Pentru toate entitățile, prima auditare IT se va realiza cel mai târziu până la data de 31 decembrie 2016.

Art. 17. — (1) La data de 1 iulie 2015 se abrogă Instrucțiunea nr. 2/2011 privind auditarea sistemelor informatice utilizate de entitățile autorizate, reglementate și supravegheate de Comisia Națională a Valorilor Mobiliare, aprobată prin Ordinul Comisiei Naționale a Valorilor Mobiliare nr. 10/2011, publicată în Monitorul Oficial al României, Partea I, nr. 118 din 16 februarie 2011, cu modificările ulterioare.

(2) La data intrării în vigoare a prezentei norme se abrogă:

a) Dispunerea de măsuri a Comisiei Naționale a Valorilor Mobiliare nr. 19/2010[1];

b) art. 25 din Normele privind principiile de organizare a unui sistem de control intern și management al riscurilor, precum și organizarea și desfășurarea activității de audit intern la asigurători/reasigurători, aprobate prin Ordinul Comisiei de Supraveghere a Asigurărilor nr. 18/2009, publicat în Monitorul Oficial al României, Partea I, nr. 621 din 16 septembrie 2009, cu modificările și completările ulterioare;

c) orice dispoziție contrară prevederilor prezentei norme.

Art. 18. — Anexele nr. 1—3 fac parte integrantă din prezenta normă.

Art. 19. — Prezenta normă se publică în Monitorul Oficial al României, Partea I, precum și în Buletinul A.S.F. și intră în vigoare la data publicării acesteia.

Președintele Autorității de Supraveghere Financiară,
Mișu Negrițoiu

București, 23 martie 2015.
Nr. 6.

ANEXA Nr. 1

DEFINIȚII ȘI ABREVIERI

1. *acord de furnizare a serviciului la parametrii agreați (SLA)* — un acord între un furnizor de servicii IT și un client, care descrie unul sau mai multe servicii IT, documentează nivelurile de serviciu țintă agreate și specifică obligațiile furnizorului de servicii IT și ale clientului;

2. *activități de control informatic* — politici, proceduri și practici aplicate pentru atingerea obiectivelor entității și pentru îndeplinirea strategiilor de eliminare a riscurilor, concepute pentru atingerea fiecărui obiectiv de control pentru eliminarea riscului identificat;

3. *arhivare electronică* — stocarea documentelor în format digital;

4. *amenințări* — capacități, strategii, intenții sau planuri ce periclitează infrastructurile, materializate prin atitudini, gesturi, acte sau fapte cu impact asupra securității activității entităților și a integrității sectorului în care activează;

5. *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 si operațiunilor acesteia;

6. *angajați/persoane-cheie* — persoane cu funcții de conducere/persoane relevante/persoane semnificative care au atribuții și răspunderi cu privire la planificarea, conducerea și controlarea activităților entității;

7. *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;

8. *audit informatic (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, asigură funcționalitățile necesare cerințelor de afaceri și respectarea legislației în

[1] Dispunerea de măsuri a Comisiei Naționale a Valorilor Mobiliare nr. 19/2010 nu a fost publicată în Monitorul Oficial al României, Partea I.

domeniu, este securizat, menține integritatea datelor prelucrate și stocate, permite atingerea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;

9. *auditor (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;

10. *audit IT cu resurse interne* — audit care se realizează de personal certificat în domeniul auditării IT, angajat în cadrul entității sau în cadrul unei companii din cadrul aceluiași grup financiar, prin aplicarea prevederilor prezentei norme și a metodologiilor certificate internațional;

11. *bază de date* — structură de organizare a informației într-unul sau mai multe domenii de aplicare, cu scopul de a o face accesibilă în permanență către utilizatori prin ansamblul de programe informatice;

12. *bune practici* — activități sau procese certificate care au fost folosite cu succes în mai multe organizații și au căpătat o largă recunoaștere, precum SR ISO/IEC 27002, ISO 20.002, cadrul de lucru și metodologiile ISACA — COBIT, RiskIT, dar fără a se limita la acestea;

13. *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);

14. *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;

15. *centrul principal de date* — centru de date care asigură serviciile IT și procesează în mod curent datele, tranzacțiile și operațiunile entității;

16. *CERT/Echipă sau centru de răspuns la incidente de urgență aferente securității informatice* — structură organizațională specializată în vederea colectării, analizării, identificării, prevenirii și reacției la incidente cibernetice cu impact semnificativ;

17. *ciclu 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;

18. *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;

19. *COBIT/Obiective de Control pentru Tehnologia Informațiilor și Tehnologii Conexe* — furnizează îndrumare și bună practică pentru managementul controalelor proceselor IT, fiind publicat de către ISACA în colaborare cu IT Governance Institute (ITGI);

20. *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;

21. *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;

22. *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;

23. *disponibilitate* — capabilitatea unui serviciu IT sau unui element de configurație IT de a efectua funcțiile agreate atunci când este necesar acest lucru;

24. *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;

25. *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;

26. *externalizare în lanț* — externalizare în cadrul căreia furnizorul extern subcontractează cu alți furnizori externi elemente componente ale serviciilor prestate entității;

27. *factori de risc* — situații, împrejurări, elemente, condiții sau conjuncturi interne și externe, uneori dublate și de acțiune, ce determină ori favorizează materializarea unei amenințări la adresa infrastructurilor importante, în funcție de o vulnerabilitate determinată, generând efecte de insecuritate;

28. *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;

29. *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;

30. *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;

31. *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;

32. *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;

33. *indicatori-cheie de risc (KRI)* — parametrii 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;

34. *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;

35. *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;

36. *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;

37. *infrastructură esențială/critică* — un sistem informatic sau o componentă a acestuia, care este esențial pentru menținerea funcțiilor infrastructurii financiare, a căror perturbare afectează semnificativ buna funcționare a acesteia, cu un impact semnificativ ca urmare a incapacității de a menține respectivele funcții;

38. *infrastructură importantă* — sistem informatic propriu sau externalizat, care asigură funcționarea activităților și serviciilor principale ale entității;

39. *integritate* — păstrarea datelor electronice, digitalizate, nealterate pe timpul comunicației dintre corespondenți sau pe perioada de stocare a datelor;

40. *internet* — rețea internațională de calculatoare, formată prin interconectarea rețelelor globale (Wide Area Network — WAN) independente (particulare, comerciale, academice sau guvernamentale), destinată facilitării schimbului de date și informații între utilizatori;

41. *ISACA* — Asociația de Audit și Control al Sistemelor Informatice/ Information Systems Audit and Control Association;

42. *SR ISO/IEC 27001* — standard care stabilește cerințele pentru un sistem de management al securității informației;

43. *SR ISO/IEC 27002* — cod de practică internațională pentru managementul securității informației, având specificația SR ISO/IEC 27001;

44. *ISO/IEC 20000* — standard care stabilește cerințele pentru un sistem de management al serviciilor IT, bazat pe setul de publicații de bune practici al Bibliotecii pentru Infrastructura IT/IT Infrastructure Library — ITIL;

45. *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;

46. *nerepudiere* — atribut care să prevină posibilitatea unei entități de a nega o acțiune întreprinsă în context informațional;

47. *obiectiv de control (informatic)* — scop și mijloc care se reflectă în punctele de control din care se extrag indicatori-cheie de risc;

48. *persoane* — investitori, brokeri de asigurare, agenți de asigurare, furnizori externi de servicii, alți terți sau colaboratori ai entității, angajați proprii — pe perioadă nedeterminată, respectiv determinată; participanți la fondurile de pensii private. Entitățile vor raporta defalcat pe fiecare tip de „persoane” în funcție de specificul activității proprii;

49. *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;

50. *portofolii, tranzacții și active* — conturile proprii ale investitorilor pe piața de capital sau ale clienților societăților de asigurări; portofolii de investitori, asigurați, operațiuni cu activele investitorilor, activele proprii ale intermediarului și/sau ale persoanelor relevante;

51. *program informatic (aplicație)* — ansamblu de instrucțiuni care poate fi executat de un sistem informatic în vederea obținerii unui rezultat determinat;

52. *resurse informaționale* — totalitatea informațiilor și a documentelor, conform cerințelor stabilite de legislația în domeniu;

53. *rețea* — ansamblu de echipamente legate între ele prin canale de transmisie, precum, dar fără a se limita la, o rețea de calculatoare;

54. *risc de securitate* — orice circumstanță sau eveniment care are un efect negativ potențial asupra securității sistemelor informatice;

55. *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;

56. *riscuri semnificative* — riscuri cu impact însemnat asupra situației financiare, patrimoniale și/sau reputaționale a entităților;

57. *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;

58. *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;

59. *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;

60. *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;

61. *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;

62. *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 agreat de serviciu (SLA);

63. *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;

64. *sistem informatic/program informatic important (aplicații core business)* — sistem/program informatic esențial pentru derularea în bune condiții a activității autorizate/avizate de Autoritatea de Supraveghere Financiară *(A.S.F.)* și pentru asigurarea raportărilor către A.S.F. sau folosite în activitatea financiar-contabilă a entității;

65. *software* — toată gama de produse program, care cuprinde cel puțin următoarele elemente: sisteme de operare, drivere sau programe informatice;

66. *soluție informatică* — un produs de tip sistem informatic, o combinație de produse sau o combinație de produse și servicii informatice care sunt furnizate de un producător sau furnizor de servicii informatice sau de comunicații;

67. *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;

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

69. *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 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	Categoria 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)	Teste de penetrare	x	x		
9	Management continuitate	x	x	x	
C) Puncte de control și măsură					
a)	Controale generale	x	x	x	
b)	Controale program informatic	x	x		
c)	Controale flux financiar	x	x	x	x

	Activitate	Categoria de risc a entității			
		Majoră	Importantă	Medie	Scăzută
D) Implementare indicatori-cheie de performanță (KPI)		x			
E) Implementare indicatori-cheie de risc (KRI)		x	x		
F) Managementul securității sistemului informatic					
a)	Măsuri organizatorice	x	x		
b)	Proceduri de securitate	x	x	x	x
c)	Evaluare securitate	x			
d)	Plan de cooperare	x	x	x	x

ANEXA Nr. 3

Indicatori de raportare electronică anuală

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

a) conform prevederilor art. 14 alin. (4) din 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;

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.

Indicatori de raportat:

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 INIȚIATE 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 neaprobate
	Număr incidente declarate aferente pierderii de date (date electronice)

1	2
	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 agreate interne și pentru clienți	
	Număr 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

EDITOR: GUVERNUL ROMÂNIEI

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București
și IBAN: RO12TREZ7005069XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București
(alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro
Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,
bloc P33, parter, sectorul 5, tel. 021.401.00.70, fax 021.401.00.71 și 021.401.00.72
Tiparul: „Monitorul Oficial” R.A.

MONITORUL OFICIAL

5 948368 829183

Monitorul Oficial al României, Partea I, nr. 227/3.IV.2015 conține 16 pagini. Prețul: 3,20 lei **ISSN** 1453—4495