PROIECT

NORMĂ
pentru modificarea și completarea Normei Autorității de Supraveghere Financiară nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară

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

în urma deliberărilor Consiliului Autorității de Supraveghere Financiară din ședința din data de 2021,

Autoritatea de Supraveghere Financiară emite prezenta normă

Art. I. – 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, publicată în Monitorul Oficial al României, Partea I, nr. 233 din 16 martie 2018 cu modificările ulterioare, se modifică și completează după cum urmează:

1. **La articolul 2, după litera k) se introduce o nouă literă, litera l), cu următorul cuprins:**

*"*l) administratorii fondurilor de pensii ocupaționale".

2. **La articolul 15 alineatele (2) și (3) se modifică și vor avea următorul cuprins:**

"(2) Entităţile au obligaţia ca, anual, să efectueze o scanare de vulnerabilităţi prin intermediul căreia trebuie evaluat și modul în care au fost soluționate vulnerabilitățile constatate anterior în cadrul exercițiilor similare.

(3) Testele de penetrare regăsite în tabelul din anexa nr. 2 la lit. B) pct. 8 lit. c) au drept obiectiv testarea securităţii aplicaţiilor incluse în scopul auditului IT, testarea securităţii sistemelor de operare utilizate în cadrul entităţii şi testarea securităţii infrastructurii reţelei, precum şi evaluarea procesului de monitorizare a activității efectuată de către societate în vederea monitorizării securității IT.*"*

3. La articolul 15 după alineatul (4) se introduce un nou alineat, alineatul (4^1) și va avea următorul cuprins:

"(4^1) În executarea obligației prevăzută la alin. (4) entitățile trebuie să se asigure că persoanele care efectuează testarea dețin cel puțin una dintre următoarele certificări: CEH – Certified Ethical Hacker, GPEN - GIAC Certified Penetration Tester, GWAPT - GIAC Web Application, LPT - Licensed Penetration Tester, OPST - OSSTMM Professional Security Tester Accredited Certification, OSCE - Offensive Security Certified Expert, OSCP - Offensive Security Certified Professional, PTC - MILLE2 Certified Penetration Testing Consultant, CPT – Certified Penetration Tester, GIAC - Penetration Tester (GPEN), GIAC - Web Application Penetration Tester (GWAPT), GIAC - Exploit Researcher and Advanced Penetration Tester (GXPN), GIAC - Mobile Device Security Analyst (GMOB), GIAC - Assessing and Auditing Wireless Networks (GAWN), CREST - Certified Simulated Attack Specialist, CSX - Cybersecurity Nexus."

4. La articolul 15 după alineatul (5) se introduce un nou alineat, alineatul (6) și va avea următorul cuprins:

"(6) Entitățile au obligația de a notifica A.S.F. cu privire la incidentele cibernetice importante apărute la nivelul sistemelor informatice".

5. Articolul 39 se modifică și va avea următorul cuprins:

" Art. 39 - (1) În vederea înscrierii în lista prevăzută la art. 38, auditorul IT extern depune la A.S.F. cererea prevăzută în anexa nr. 5, însoţită de documentaţia care trebuie să cuprindă următoarele, după caz:

1) Pentru auditorul IT extern persoană fizică autorizată care va semna raportul de audit, se depun următoarele documente:

a) actul de identitate al auditorului IT, în copie;

b) curriculum vitae în format Europass, datat şi semnat, în care se precizează studiile și cursurile de formare relevante, experienţa profesională în auditarea IT a sistemelor informatice, natura și durata atribuțiilor îndeplinite;

c) certificatul CISA emis de ISACA în termenul de valabilitate, în copie, semnată pentru conformitate cu originalul;

d) scrisori de recomandare, care să ateste experienţa în domeniul de audit IT extern al sistemelor informatice, incluzând datele de contact ale persoanelor care pot oferi referințe;

e) certificatul de cazier judiciar și certificatul de cazier fiscal în original, în termenul de valabilitate;

f) contract de asigurare de răspundere civilă profesională, pentru suma asigurată de minimum 100.000 euro, în vigoare, în copie;

g) documentul de plată a tarifului de înscriere în lista prevăzută la art. 38, în copie;

2) pentru auditorul IT extern - persoană juridică, se depun următoarele documente:
a) certificat constatator emis de Oficiul Naţional al Registrului Comerţului, cu starea la zi a persoanei juridice, în original;
b) actul de identitate al reprezentantului legal al auditorului IT extern - persoană juridică, în copie;
c) decizia/hotărârea organului statutar al societății de numire a coordonatorului societății de audit IT care va semna în numele și pe seama societății de audit IT, raportul de audit:
i) auditori IT din cadrul societății (salariați proprii, reprezentant legal sau membrii conducerii societății);
ii) auditor IT, persoană fizică cu care societatea a încheiat un contract de prestări servicii pentru a întocmi raportul de audit în numele și pe seama societății;
d) contract de prestări servicii încheiat cu persoana menționată la lit. c) pct. ii) care va semna în numele și pe seama societății raportul de audit, în copie;
e) documentele prevăzute la secțiunea A) lit. a) - e) pentru coordonatorul certificat al societății de audit IT persoană fizică menționat în decizia/hotărârea organului statutar menționată la lit. c);
f) contract de asigurare de răspundere civilă profesională pentru suma asigurată de minimum 100.000 euro, în vigoare, în copie;
g) documentul de plată a tarifului de înscriere în lista prevăzută la art. 38, în copie.
(2) Documentele care nu sunt emise limba română se depun în copie, împreună cu traducerea legalizată a acestora.
(3) Pentru documentele depuse în copie, în vederea asigurării conformității cu originalele, acestea sunt semnate de auditorul IT persoană fizică, respectiv de reprezentantul legal al auditorului IT persoană juridică, după caz.”

6. Articolul 41 se modifică și va avea următorul cuprins:

“Art. 41 - Orice modificare a documentaţiei prevăzute la art. 39 pct. 1 lit. a), c), e) și f), pct. 2 lit. a)-f) trebuie transmisă A.S.F. în termen de maximum 30 de zile de la data efectuării modificării.”

7. Articolul 43 se modifică și va avea următorul cuprins:

“Art. 43. (1) Pentru toate situaţiile menţionate la art. 42 lit. c) și d), A.S.F. transmite auditorului IT extern o notificare prealabilă prin care i se aduc la cunoştinţă faptele pentru care A.S.F. va proceda la iniţierea demersurilor pentru radierea din Lista auditorilor IT externi.

(2) În situațiile în care A.S.F. nu poate contacta auditorul IT extern care se află într-unul dintre cazurile menționate la art. 42 lit. b) sau acesta nu transmite informațiile solicitate în conformitate cu prevederile art. 41, pentru clarificarea situației informațiile necesare se solicită la Oficiul Național al Registrului Comerțului.”

8. La articolul 46 alineatul (1), punctul 4 al literei d) se modifică și va avea următorul cuprins:

"4. Informații doveditoare referitoare la valoarea disponibilității măsurată pe parcursul auditului;"

9. La articolul 48, partea introductivă se modifică și va avea următorul cuprins:

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

10. Articolul 55 se modifică și va avea următorul cuprins:

„Art. 55 - Anexele nr. 1-5 fac parte integrantă din prezenta normă."

11. La anexa nr. 1, punctul 5 se modifică și va avea următorul cuprins:

"5. auditor IT extern – persoană care derulează o activitate de auditare a sistemelor informatice, conform reglementărilor și bunelor practici în domeniu precum:
i) persoana fizică autorizată care deţine certificatul CISA emis de ISACA,
ii) persoană juridică cu personal propriu care deţine certificatul CISA emis de ISACA sau, după caz, cu contract de prestări servicii încheiat cu o persoană fizică, care deţine certificatul CISA emis de ISACA, care va semna în numele și pe seama seama societății raportul de audit în calitate de coordonator."

12. La anexa nr. 1, după punctul 9 se introduce un nou punct, punctul 9^1 cu următorul cuprins:

"9^1. CISA- Auditor Certificat de Sisteme Informatice/Certified Information Systems Auditor."

13. La anexa nr. 3 punctul I, Raportul de audit IT, coloana Capitol, literele F și G se modifică și vor avea următorul cuprins:

"F Datele de identificare ale coordonatorului certificat al echipei de audit IT extern persoană juridică/auditorului IT extern persoană fizică autorizată/auditor IT intern certificat al entității auditate

G Semnătura coordonatorului certificat al echipei de audit şi semnătura reprezentantului legal al auditorului IT extern persoană juridică/semnătura auditorului IT extern persoană fizică autorizată/semnătura auditorului IT intern certificat al entității auditate. "

14. La anexa nr. 3 punctul II Anexe la raportul de audit IT, punctul 7 se modifică și va avea următorul cuprins:

"7. Declaraţie pe propria răspundere a reprezentantului legal al entităţii auditate IT cu resurse interne.
Anexa conţine informaţii cu privire la efectuarea auditului IT cu resurse interne certificate care sunt independente faţă de activitatea auditată şi certificatul CISA emis de ISACA în termenul de valabilitate, în copie, semnată pentru conformitate cu originalul. "

15. După anexa nr. 4 se introduce o nouă anexă, anexa nr. 5 având cuprinsul prevăzut în anexa nr. 1 care face parte integrantă din prezenta normă.

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

Art. III. – Prezenta normă se publică în Monitorul Oficial al României, Partea I și intră în vigoare la data publicării.

Președintele Autorității de Supraveghere Financiară,

Nicu MARCU

București, _____
Nr. _____

Anexa nr. 1

Anexa nr. 5 la Norma A.S.F. nr. 4/2018

CERERE

pentru înscrierea în Lista auditorilor IT externi menținută de A.S.F.

1. Denumirea completă/numele complet: .....
2. Sediul social……..
3. Adresa unde îşi desfăşoară activitatea: .....
4. Numărul de telefon .....
5. Numărul de fax .....
6. Adresa de e-mail .....
7. Reprezentantul legal .....
8. Adresa paginii de internet .....
9. Opisul documentelor depuse în anexa la cerere în conformitate cu art. 39 din Norma nr. 4/2018 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile autorizate/avizate/înregistrate, reglementate şi/sau supravegheate de către Autoritatea de Supraveghere Financiară**.**

Subsemnatul[1] ……., cunoscând dispozițiile art.326 Cod Penal cu privire la falsul în declarații, declar pe propria răspundere că toate informațiile furnizate sunt corecte, complete şi conforme cu realitatea;
Totodată, menționez că sunt de acord cu prelucrarea datelor personale[2] în scopul exercitării atribuțiilor A.S.F. și mă angajez să comunic A.S.F. toate modificările privind informațiile furnizate.

Data Semnătura

[1] Se completează numele și prenumele auditorului IT persoană fizică/ reprezentantului legal al auditorului IT persoană juridică astfel cum apare în actul de identitate
[2] Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE