

## REFERAT

### **cu privire la proiectul normei de modificare și completare a Normei 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**

Norma nr. 4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară, este un act normativ integrat care reglementează activitățile și operațiunile pentru evaluarea, supravegherea și controlul riscurilor operaționale generate de utilizarea sistemelor informatice, precum și gestionarea riscurilor privind securitatea sistemelor informatice importante utilizate de către entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către A.S.F..

Prin proiectul normei de modificare și completare a Normei nr. 4/2018 sunt aduse modificări și completări care sunt fundamentate în baza aspectelor practice desprinse din aplicarea normei menționate, astfel încât prin adaptarea acesteia la cerințele contextului existent să se asigure o gestionare eficientă a riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către A.S.F..

Modificarea și completarea Normei nr. 4/2018 vizează o serie de aspecte, cum ar fi:

- precizarea tipului de certificare specifică pe care trebuie să o dețină un auditor IT extern pentru a fi eligibil în ceea ce privește capacitatea de a efectua teste de penetrare, astfel încât să răspundă cerințelor misiunii de audit IT;
- instituirea obligației pentru entitățile reglementate de a notifica A.S.F. cu privire la incidentele cibernetice importante apărute la nivelul sistemelor informatice;
- reglementarea situațiilor în care auditorul IT extern care a intrat în lichidare/insolvență nu transmite informațiile solicitate de către A.S.F. sau nu poate fi contactat;
- reconsiderarea conținutului notificării referitoare la externalizarea unor servicii IT ce urmează a fi transmisă la A.S.F., având în vedere situațiile concrete semnalate de entități;
- reformularea unor condiții pe care trebuie să le îndeplinească auditorul IT extern persoană fizică/juridică pentru a figura în *Lista auditorilor IT externi menținută de A.S.F.*, concomitent cu redefinirea documentelor care trebuie depuse la A.S.F. în acest scop;
- introducerea unui format standardizat pentru transmiterea cererii de înscriere a auditorilor IT externi în *Lista auditorilor IT externi menținută de A.S.F.*, în scopul eficientizării procesului ;
- definirea CISA și modificarea definiției auditorului IT extern.