NOTĂ DE FUNDAMENTARE

Proiectul de normă vizează o îmbunătățire a abordării privind gestionarea riscurilor operaționale generate de sistemele informatice plecând de la elementele de noutate aduse de auditul IT, propunerile primite și concluziile desprinse cu ocazia întâlnirilor cu auditorii IT, precum și propunerile bazate pe cazurile concrete cu care s-a confruntat autoritatea.

În acest context, în proiectul de normă au fost incluse unele aspecte esențiale pentru tratarea riscurilor cibernetice. Astfel, ca principale soluții care să conducă la creșterea rezilienței și la reducerea vulnerabilităților a fost statuată obligația efectuării unei scanări de vulnerabilități de către toate entitățile care intră sub incidența normei, a fost definit scopul testelor de penetrare și a fost extinsă obligația efectuării acestora la entitățile din categoria de risc mediu (toate SSIF-urile, principalele SAI-uri și fondurile de garantare), precum și obligația testării anuale a planului de răspuns la incidente de securitate informatică, elaborarea unui raport care să cuprindă rezultatele testării și prezentarea acestuia auditorului IT.

Un alt element de noutate în proiectul de normă îl reprezintă definirea sistemelor informatice importante deținute de o entitate care vor fi supuse auditului IT, însoțită de concentrarea ariei de cuprindere a normei asupra acestor sisteme informatice, dar și instituirea obligației în sarcina entității de a audita IT orice sisteme informatice în anumite situații bine determinate, precum atunci când activitățile desfășurate de către aceasta au un caracter formal, sau când autoritatea apreciază că se impun investigații suplimentare la nivelul sistemelor informatice sau efectuarea unui audit IT la acele sisteme IT pe care entitatea le va dezafecta.

Totodată, s-a instituit în sarcina entității obligația de a se asigura că furnizorii de servicii IT externalizate permit auditorului IT și autorității să verifice și/sau auditeze sistemele sale informatice în contextul aplicării prevederilor normei sau că aceștia pun la dispoziția auditorului IT un raport de audit IT întocmit în conformitate cu standardul ISAE 3402.

Alte elemente de noutate regăsite în proiectul de normă sunt reprezentate de introducerea unei machete de raportare privind elementele minime care trebuie incluse în raportul de audit, includerea în macheta de raportare a obligației de verificare de către auditorul IT a implementării măsurilor constatate la misiunea anterioară de audit IT, precum și introducerea obligației auditorului IT de a întocmi și de a prezenta conducerii entității auditate o situație a deficiențelor și vulnerabilităților identificate.

În fapt, proiectul de normă a urmărit identificarea celor mai bune practici în materie de audit IT și aplicarea acestora în activitatea de audit IT, astfel încât să se răspundă noilor provocări în materie de audit IT și de gestionare a riscurilor generate de sistemele informatice.