Revista Universul Juridic ● nr. 2, februarie 2022, pp. 90-101

TENDINȚE ACTUALE ÎN ACTIVITATEA DE AUDIT. AUDITUL SISTEMELOR INFORMATICE

Ramona CIOBANU
Facultatea de Drept
Universitatea „Transilvania" din Braşov

Abstract

The implementation of information systems has entailed the emergence of a new type of audit, namely the information systems audit, which mainly aims at establishing the degree of credibility of the computerized system. By identifying the risks and vulnerabilities to which the system is exposed, auditing significantly contributes to increasing cybersecurity.

Keywords: *audit, digitization, cybersecurity, information systems auditing*

1. Considerații introductive privitoare la audit

Din punct de vedere etimologic, cuvântul *audit* provine din latinescul *audire*, care înseamnă a asculta, a audia. Astăzi, acest termen este utilizat cu sensul de a verifica, a examina, a revizui.

Activitatea de audit – de verificare şi examinare – este strâns legată de activitatea economică, de producție, comerț şi deci de schimb, explicația rezidând în aceea că desfăşurarea şi succesul acestor activități sunt greu de imaginat fără înregistrarea operațiunilor efectuate, a fluxurilor financiare, a intrărilor şi ieşirilor de bunuri şi monedă, fără o evidență a stocurilor şi disponibilităților financiare, a activului şi pasivului. Astfel, întocmirea şi ținerea unor registre şi conturi privind operațiunile efectuate, controlul acestor registre şi conturi privind corectitudinea înregistrărilor şi apoi auditul activității desfăşurate, ca formă superioară de control având ca scop detectarea erorilor şi a fraudelor, reprezintă premise pentru eficiența activității desfăşurate. Iată de ce activitățile de control şi cele incipiente de audit le găsim încă în antichitate, spre exemplu cu privire la fondurilor publice în Egipt, Grecia, Mesopotamia, Roma.

Dezvoltarea ulterioară a manufacturilor, perfecționarea mijloacelor de navigație, descoperirile geografice, Revoluția industrială sunt evenimente care au amplificat activitatea comercială, problema înregistrărilor şi a controlului acestor înregistrări punându-se din ce în ce mai acut. Revirimentul produs de Renaştere a avut impact şi asupra acestor din urmă activități, astfel încât Luca Pacioli, în lucrarea *Summa di Arithmetica, Geometria, Proportioni et Proportionalita*, publicată la Veneția în anul 1494, a stabilit reguli pentru corecta utilizare a registrelor contabile şi a expus pentru prima dată metoda contabilității în partidă dublă, numită „metoda Veneției" („modo di Venetia") contribuții pentru care este considerat părintele contabilității. În această lucrare de matematică aplicată, Pacioli a evidențiat caracterul general al aplicabilității acestei metode, precum şi faptul că pentru creşterea eficienței acesteia trebuie respectate principiile etice de ordine, claritate şi credibilitate[1].

Revoluția industrială a influențat semnificativ evoluția auditului, simțindu-se din ce în ce mai mult nevoia existenței unor persoane specializate în domeniul contabilității şi auditului şi, în consecință, nevoia existenței unor instituții care să formeze aceşti specialişti şi să-i autorizeze, demersuri care aveau menirea să le crească prestigiul profesional, încrederea în competențele şi corectitudinea lor. Astfel, au fost constituite, spre exemplu, Institutul Contabililor Autorizați din Anglia şi Țara Galilor (1880) şi Asociația Britanică a Contabililor şi Auditorilor (1923)[2].

Aşadar, inițial activitatea de audit a privit conturile, finanțele private, dar şi cele publice, astfel încât în etapa de început a auditului putem vorbi despre audit contabil, audit financiar şi audit fiscal sau despre accepțiunea *lato sensu* a auditului financiar ca activitate care înglobează şi auditul contabil şi fiscal. Ulterior s-a simțit nevoia auditării şi a altor domenii, fapt care a determinat apariția unor noi forme de audit.

Nu există o definiție unanim acceptată a noțiunii de audit, dar în literatura de specialitate[3] este des citată definiția dată de Asociația Americană de Contabilitate care în cadrul *Declarației privind conceptele de bază ale auditului*[4], adoptată în 1973, precizează că„auditul este un proces sistematic de obținere şi evaluare obiectivă a unor afirmații privind acțiunile şi evenimentele cu caracter economic, în vederea aprecierii gradului de conformitate a acestor afirmații cu criteriile prestabilite, precum şi de comunicare a rezultatelor către utilizatorii interesați".

---

[1] Pentru detalii, a se vedea Massimo Ciambotti, *Luca Pacioli, la Partita Doppia e la storia della contabilità e della società,* Centro Studi Mario Pancrazi, https://www.centrostudimariopancrazi.it/images/pubblicazioni/before_and_after_luca_pacioli/9.pdf.

[2] V. Kumar, *Auditing. Basic concepts of auditing,* pp. 7-11, https://prgc.ac.in/uploads/study_material/5th%20sem%20I%20Unit%20Auditing%20PPT-1.pdf334.pdf, accesat în 10.02.2022 .

[3] P. Năstase (coordonator) ş.a., *Auditul şi controlul sistemelor informaționale*, Ed. Economică, Bucureşti, 2007, p. 14.

[4] American Accounting Association, Committee on Basic Auditing Concepts, *A Statement of Basic Auditing Concepts,* Sarasota, FL: American Accounting Association, 1973.

În literatura de specialitate din România[5], *auditul* a fost definit ca fiind procesul desfăşurat de persoane fizice sau juridice legal abilitate, numite auditori, prin care se analizează şi se evaluează, în mod profesional, informaţii legate de o anumită entitate, utilizând tehnici şi procedee specifice, în scopul obţinerii de dovezi, numite probe de audit, pe baza cărora auditorii emit într-un document, numit raport de audit, o opinie responsabilă şi independentă, prin apelarea la criterii de evaluare care rezultă din reglementările legale sau din buna practică recunoscută unanim în domeniul în care îşi desfăşoară activitatea entitatea auditată.

Pornind de la această definiţie, distingem *elementele specifice auditului*:

- *procesul de audit* sau *misiunea de audit* se desfăşoară cu respectarea unor standarde naţionale şi internaţionale;
- *auditorii* sunt specialiştii în audit, autorizaţi conform legislaţiei în vigoare să desfăşoare această activitate;
- *entitatea auditată* poate fi: o societate colectivă (societate comercială, fond de investiţii, regie autonomă, companie naţională etc.), Guvernul, ministerele, alte instituţii publice publice sau private, dar şi programe sau acţiuni;
- obţinerea informaţiilor în cadrul misiunii de audit se realizează cu ajutorul unor *procedee şi tehnici* unanim recunoscute în domeniu, care furnizează auditorului *probe de audit*, pe baza cărora auditorul îşi formulează opinia de audit în cadrul *raportului de audit*; sunt folosite documente şi informaţii obţinute din interiorul entităţii auditate, coroborate cu informaţii din alte surse.
- ca şi în cazul obţinerii informaţiilor, *evaluarea şi interpretarea rezultatelor auditului* se realizează pe baza unor criterii stabilite în legislaţia naţională, standarde naţionale şi internaţionale, proceduri specifice naţionale şi internaţionale, ghiduri de bune practici în domeniu.

Trebuie să facem distincţie între control şi audit. Esenţa auditului nu este controlul. Noţiunea de control provine din expresia latină *contra rolus* care înseamnă verificarea actului original după duplicatul care se încredinţează în acest scop altei persoane. Controlul este activitatea prin care se stabileşte exactitatea operaţiunilor materiale, control care se afectuează înainte (control preventiv), concomitent (control concomitent) sau după desfăşurarea acestor operaţiuni (control ulterior)[6]. Auditul este o activitate superioară de *orientare, analiză şi de sinteză*, iar auditorii sunt persoane cu înaltă calificare profesională care nu se substituie controlorilor.

Fundamentele teoriei auditului sunt: postulatele, conceptele, standardele, procedurile.

---

[5] M. Boulescu, M. Ghiţă, V. Mareş, *Fundamentele auditului*, Ed. Didactică şi Pedagogică, Bucureşti, 2001, p. 11.

[6] D. D. Şaguna, D. Şova, *Drept financiar public*, Ed. All Beck, Bucureşti, 2005, pp. 246-248.

Postulatele reprezintă un ansamblu de premise, principii, condiţii, ipoteze considerate adevărate fără a fi demonstrate şi care constituie baza elaborării standardelor de audit. Exemple de postulate în acest sens ar putea constitui reducerea riscului apariţiei erorilor şi fraudelor prin organizarea unui control intern performant, analiza tuturor situaţiilor care apar pe parcursul auditării şi evitarea apariţiei conflictului de interese între auditor şi entitatea auditată.

Conceptele sunt generalizări, idei centrale, fundamentale pentru raţionamentul teoretic, deduse din postulatele unui anumit tip de audit şi se referă la probele de audit, corectitudinea raportării, independenţa şi conduita etică a auditorului, respectarea profesiei de auditor.

Standardele de audit sunt caracterizate prin gradul ridicat de conceptualizare, ele aflându-se la baza îndeplinirii unei misiuni de audit. Standardele asigură criteriile pentru îndeplinirea şi evaluarea activităţii de audit, crează premisele comportamentului profesional al auditorilor, susţinând totodată credibilitatea şi prestigiul auditorilor. *Standardele naţionale de audit* reprezintă un set de norme privind activitatea de audit, stabilite prin lege sau alte acte normative, inclusiv prin reglementări emise de o autoritate competentă la nivel naţional, a căror aplicare şi respectare este obligatorie pentru efectuarea unui audit sau a serviciilor conexe. Tendinţa predominantă, pe plan mondial, în domeniul auditului, o reprezintă *standardizarea*, în vederea formulării unei teorii privitoare la descrierea, explicarea şi planificarea activităţilor de audit. Vorbim aşadar despre o anumită predictibilitate în ceea ce priveşte desfăşurarea misiunii de audit, despre rigoarea care trebuie s-o caracterizeze. Standardele naţionale se fundamentează pe *standardele internaţionale de audit* adoptate în cadrul unor organizaţii internaţionale interguvernamentale sau neguvernamentale (asociaţii profesionale cu caracter internaţional).

Procedurile de audit reprezintă *ansamblul testelor* pe care auditorul le aplică pentru culegerea probelor de audit care să-i susţină opinia emisă prin raportul de audit. Ele pot fi adaptate şi modificate de auditor în funcţie de specificul entităţii auditate, alegerea, adaptarea şi modificarea procedurilor de audit ţinând exclusiv de raţionamentul şi experienţa profesională a auditorului. Evident că acesta va avea în vedere standardele de audit, cerinţele organizaţiilor profesionale relevante, legislaţia în vigoare şi clauzele contractului de audit.

Desfăşurarea auditului se realizează în temeiul *contractului de audit* care reprezintă acordul stabilit între auditor şi entitatea auditată privind obiectivul şi aria de aplicabilitate a auditului, termenul în care trebuie finalizat, preţul, alte drepturi şi obligaţii ale părţilor. Contractul de audit poate fi întâlnit şi sub denumirea de angajament de audit, scrisoare de angajament sau altă denumire convenită de părţi.

2. Tipuri de audit

Există mai multe tipuri de audit şi pentru clasificarea acestora sunt utilizate o serie de criterii.

▪ *Clasificarea în funcție de domeniul auditat*

Noțiunea de audit a fost asociată inițial domeniului financiar urmărind corectitudinea, legalitatea, eficiența şi eficacitatea operațiunilor financiare efectuate în cadrul unei instituții. Într-o accepțiune mai largă, auditul financiar include şi auditul contabil, precum şi auditul fiscal.

În prezent, noțiunea de audit este asociată unor domenii diferite, precum cel financiar, protecției mediului, capitalului intelectual, sistemelor informatice, calității, social.

▪ *Clasificare în funcție de obiectivul şi aria de aplicabilitate a auditului*

În funcție de aceste criterii putem identifica:

- auditul de conformitate/legalitate/regularitate care evaluează respectarea normelor aplicabile domeniului şi entității auditate;

- auditul performanței sau al rezultatelor care evaluează dacă rezultatele sunt conforme cu obiectivele entității auditate;

- auditul de sistem care evaluează sistemele de conducere şi control intern al entității auditate.

▪ *Clasificare în funcție de aspectul organizatoric şi funcțional*

Este vorba despre relația dintre auditor şi entitatea auditată, criteriu în funcție de care distingem:

- audit intern – efectuat de auditori interni, specializați, angajați ai entității auditate;

- audit extern sau independent - efectuat de auditori externi independenți, persoane fizice sau juridice;

▪ *Clasificare în funcție de entitatea auditată*

Este vorba despre clasificarea în funcție de sectorul căreia aparține entitatea auditată şi anume:

- audit privat – entitatea auditată este o instituție din sectorul privat (societate comercială, asociație agricolă, composesorat, fond de investiții, asociații, fundații etc.);

- audit public – entitatea auditată este o instituție publică (guvern, ministere, primării, consilii locale, instituții subordonate acestora, instituții publice autonome etc.); dacă auditul din sectorul privat este organizat şi se desfăşoară potrivit deciziilor managementului intern al instituției, desigur cu respectarea legislației şi, pentru asigurarea eficienței acestuia, prin raportare la standarde, proceduri, ghiduri, coduri etice, auditul public este reglementat prin acte normative şi trebuie să se supună dispozițiilor acestora[7].

[7] Pentru detalii privind auditul public, a se vedea D. D. Şaguna, D. Şova, *op. cit.*, pp. 264-330; Legea nr. 94/1992 privind organizarea şi funcționarea Curții de Conturi a României, modificată şi

3. Apariția şi evoluția auditului sistemelor informatice

Implementarea sistemelor informatice în toate domeniile activității umane a avut un impact deosebit asupra auditului, astfel încât acesta din urmă a trebuit să se adapteze noilor realități tehnologice şi să țină cont atât de avantajele, cât şi de riscurile specifice mediilor informatizate. Drept urmare, pe de o parte, tehnologia informației devine o resursă cheie a oricărei instituții, resursă care trebuie controlată şi auditată prin tehnici şi proceduri specifice, fapt care a condus la *apariția auditului sistemelor informatice*, iar pe de altă parte, orice tip de audit trebuie să integreze şi tehnologia informației, adoptarea tehnicilor automate de audit fiind necesară în condițiile în care sistemele auditate sunt informatizate pe o scară din ce în ce mai largă[8].

Auditorii financiari au realizat faptul că folosirea sistemelor informatice are consecințe importante asupra auditului financiar, verificarea integrității datelor devenind o etapă necesară, premergătoare îndeplinirii obiectivelor misiunii lor de audit, astfel încât rezultatele din rapoartele de audit să fie bazate pe date complete şi precise. Drept urmare, în 1968, Institutul American al Contabililor Autorizați *(American Institute of Certified Public Accountants – AICPA)* a lansat conceptul de *audit al sistemelor de procesare automată a datelor (Electonic Data processing – EDP Audit,* iar în 1969 s-a constituit Asociația Auditorilor EDP *(EDP Auditors Association – EDPAA)* care şi-a propus să elaboreze standarde, ghiduri şi proceduri pentru acest nou tip de audit.

Extinderea folosirii internetului, dezvoltarea fără precedent a afacerilor, comerțului, serviciilor bancare în mediul virtual a atras riscuri informatice specifice – fraudele şi pierderile de date – fapt care a impus dezvoltarea în cadrul fiecărei instituții a unui control intern al sistemului informatic. Managerii au fost puşi în fața unei noi probleme: garantarea corectitudinii şi securității operațiunilor din sistemul informatic. De regulă, în practică se pleacă de la premisa că informațiile generate de calculator sunt întotdeauna corecte, dar în fapt calculatorul face ceea ce este programat să facă şi fără o testare prealabilă a mecanismelor de control din mediul informatizat nu se poate concluziona că informațiile produse de sistemul informatic sunt corecte. Procedurile de control şi certificare a datelor s-au născut din această *nevoie de încredere*.

În 1994, EDPAA devine Asociația pentru Auditul şi Controlul Sistemelor Informaționale, cunoscută sub acronimul *ISACA (Information Systems Audit and Control Association)* şi recunoscută ca organizație profesională care grupează şi certifică specialişti în domeniul auditului sistemelor informatice. Conceput inițial

completată, republicată; Legea nr. 672/2002 privind organizarea auditului public intern; https://mfinante.gov.ro/domenii/informatii-contribuabili/institutii-publice/ucaapi/ghiduri-audit; https://www.curteadeconturi.ro.

[8] P. Năstase (coordonator) ş.a., *op. cit.*, pp. 14-15.

ca o extensie a auditului financiar, auditul sistemelor informatice devine un audit de sine-stătător, cu reguli şi obiective specifice.

Potrivit unor opinii din literatura de specialitate[9] trebuie să facem distincție între auditul sistemului informațional şi auditul sistemului informatic. În timp ce *auditul sistemului informațional* cuprinde prin obiectivele sale toate nivelurile sistemului informațional de la evaluarea proiectării şi utilizării sistemului informatic şi până la evaluarea politicilor şi procedurilor de securitate la nivel operațional şi strategic, auditul *sistemului informatic* sau *auditul informatic* acoperă doar sistemul informatic. Între cele două există o relație de la întreg la parte, auditul sistemului informațional cuprinzând şi auditul inforrmatic. Cu toate acestea, în mod curent se folosesc denumirile de audit al sistemelor informatice, audit informatic, audit IT, audit ŞI sau audit cibernetic pentru a desemna auditul care acoperă toate nivelurile sistemului informațional.

Auditul sistemelor informatice reprezintă activitatea de evaluare a unui sistem informatic în scopul emiterii unei opinii calificate asupra gradului de conformitate a sistemului cu standardele în domeniu şi, totodată, asupra capacității sistemului informatic de a atinge obiectivele strategice ale unei organizații, utilizând eficient resursele informaționale şi asigurând integritatea datelor prelucrate şi stocate[10].

Această activitate complexă este desfăşurată de auditorul sistemelor informatice care are pregătire în domeniul controlului, securității şi managementului sistemelor informatice şi este atestat să desfăşoare această activitate.

4. Auditul sistemelor informatice – garanție a securității mediului informatizat

Auditul sistemelor informatice poate fi organizat şi realizat în cadrul instituției, ca o componentă a *auditului intern*, dar poate fi realizat şi sub forma *auditului extern*, la solicitarea instituției, de către un auditor extern independent.

Auditul intern confirmă respectarea procedurilor de transformare a datelor de intrare în rezultate, urmărindu-se modul în care sistemul care se implementează este mai eficient, fiind însoțit de o economisire a resurselor[11].

Auditul extern include proceduri prin care se evidențiază comportamentul sistemului informatic prin *testări* cu ajutorul cărora se măsoară cât de stabile, fiabile şi mentenabile sunt procedurile de control care intră în componența sistemului, proceduri care implementeză toate cerințele exprese incluse în specificații, legi,

[9] P. Năstase (coordonator) ş.a., *op. cit.*, p. 16.

[10] *Ibidem.*

[11] I. Ivan, A. Felician, S. Capisizu, *Auditul informatic*, în Economistul, 1887/2005, p.18, http://alecu.ase.ro/articles/economistul_2005.pdf, accesat în 9.02.2022.

regulamente, standarde şi care restricționează prin blocare orice tentativă de execuție a operațiunilor interzise[12].

Se pot desfăşura următoarele *tipuri de audit al sistemelor informatice*[13]*:*

- evaluarea unui sistem informatic în scopul furnizării unei asigurări rezonabile privind funcționarea acestuia, asigurare necesară inclusiv misiunilor de audit financiar sau al performanței la care este supusă entitatea;
- evaluarea performanței implementării şi utilizării sistemelor informatice;
- misiuni de audit mixte, prin integrarea a trei tipuri de audit: auditul financiar, auditul performanței şi auditul IT, acestea urmând a se desfăşura în cadrul unor misiuni comune, în funcție de obiectivele stabilite. Extinderea utilizării tehnologiei informației în toate domeniile presupune extinderea controalelor IT în cadrul sistemului de control intern al entității auditate, generează necesitatea perfecționării modelelor tradiționale de auditare şi extinderea auditului sistemelor informatice în activitatea unității.

Auditorii sistemelor informatice sau auditorii de securitate cibernetică au următoarele *obiective*[14]:

- identificarea şi evaluarea riscurilor de sistem,
- verificarea funcțiilor incompatibile în cadrul sistemului informatic,
- verificarea securității fizice şi logice a sistemului informatic,
- verificarea şi evaluarea infrastructurii rețelelor de calculatoare,
- controlul aplicațiilor informatice,
- testarea integrității datelor,
- verificarea existenței şi securității copiilor de siguranță a datelor, informațiilor, aplicațiilor informatice,
- verificarea şi evaluarea planurilor de recuperare în caz de dezastre.

Fluxurile de informații specifice oricărui sistem informatic trebuie să asigure integritatea informațiilor, completitudinea prelucrărilor, corectitudinea rezultatelor şi mai ales accesibilitatea beneficiarului la informația aşteptată, obținând în acest fel un nivel maxim al satisfacerii cerințelor proprii. Iată de ce auditul sistemelor informatice este un demers deosebit de complex şi trebuie aşezat pe un fundament solid. Obiectivul fundamental al activității de auditare informatică este stabilirea gradului de credibilitate a sistemului informatizat de management[15].

Un sistem informatic, fie că este un sistem general pentru managementul organizației sau unul special destinat managementului financiar, trebuie înzestrat, atât cu funcțiile clasice de prelucrare şi de extragere a rezultatelor, de creare şi

---

[12] *Ibidem*.

[13] I. F. Chiş, L. S. Tudor, *Auditul sistemelor informatice*, în Conferința Academia Comercială Satu Mare 2014, p. 143, http://conferinta.academiacomerciala.ro/CD2014/articole/2/AUDITUL%20SISTEMELOR%20INFORMATICE%20Chis%20Todor.pdf, accesat în 9.02.2022.

[14] P. Năstase (coordonator) ş.a., *op. cit.*, p. 17.

[15] I. Ivan, A. Felician, S. Capisizu, *op. cit.*, pp. 17-18.

actualizare a bazei de date, cât şi cu *funcții de management pentru calitatea şi protecția sistemului informatic însuşi.* Pe măsura creşterii complexității proceselor din societatea informațională, utilizarea sistemelor informatice impune un nivel de credibilitate deosebit de ridicat pe care numai auditul informatic îl poate susține cu succes[16].

5. Legislația din România privitoare la mediul informatizat

În ultimii ani, ținând cont tendințele din economia mondială, de digitizare şi digitalizare, de folosirea sistemelor informatice pe scară din ce în ce mai largă în toate sectoarele economiei şi domeniile de activitate, precum şi de faptul că România trebuie să fie conectată la realitățile internaționale şi să țină pasul cu ele, în țara noastră au fost adoptate numeroase *reglementări privind mediul informatizat*. Cu titlu de exemplu enumerăm:

- Legea nr. 455/2001 privind semnătura electronică,
- Legea nr. 365/2002 privind comerțul electronic,
- Legea nr. 506/2004 privind protecția datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice,
- Legea nr. 102/2005 privind înființarea, organizarea şi funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal,
- Legea nr. 64/2004 pentru ratificarea Convenției privind criminalitatea informatică adoptată în cadrul Consiliului Europei,
- *H.G. nr. 271/2013 pentru aprobarea Strategiei de Securitate Cibernetică a României (SNSC) şi a Planului de acțiune la nivel național privind implementarea SNSC,*
- *Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice* denumită şi *Legea NIS* şi care transpune în legislația internă *Directiva UE 2016/1148 (NIS) a Parlamentului European şi a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor şi a sistemelor informatice în UE,*
- *Ordinul nr. 559/2021 privind aprobarea Regulamentului pentru atestarea şi verificarea auditorilor de securitate cibernetică,*
- *O.U.G. nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică,*

Totodată, în România au fost adoptate şi standarde referitoare la securitatea informațională/cibernetică, precum:

- ISO/IEC 27001:2005 Tehnologia Informației – Tehnici de securitate – Sisteme de management al informațiilor – Cerințe care priveşte managementul securității informației, contribuind la minimizarea amenințărilor care afectează informația;

[16] I. Ivan, A. Felician, S. Capisizu, *op. cit.*, p. 19.

▪ ISO/IEC 17799 Tehnologia informației – Cod de bună practică pentru managementul securității informației – care reprezintă un ghid pentru implementarea unor politici, practici şi proceduri pentru consolidarea securității informației gestionate de o entitate.

6. Instituții publice cu atribuții în asigurarea securității sistemelor informatice

Coordonarea strategică la nivel național a activităților de asigurare a unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice se realizează de către **Guvern,** prin Ministerul Comunicațiilor şi Societății Informaționale sub aspectul politicilor publice şi al inițiativei legislative în domeniu.

*Strategia națională privind securitatea rețelelor şi a sistemelor informatic*e se aprobă, prin hotărâre a **Guvernului**, la propunerea Directoratului Național de Securitate Cibernetică.

Ministerul Comunicațiilor şi Societății Informaționale este instituția de specialitate a administrației publice centrale în domeniul comunicațiilor şi tehnologiei informației, care are rolul de a realiza politica Guvernului în domeniile comunicațiilor electronice, serviciilor poştale, tehnologiei informației şi societății informaționale. Ministerul are ca misiune crearea premiselor trecerii la societatea informațională din România. Sub coordonarea sa îşi desfăşoară activitatea *Institutul Național de Cercetare-Dezvoltare în Informatică* şi *Agenția pentru Agenda Digitală a României.*

Ministerul Cercetării, Inovării şi Digitalizării în structura căruia funcționează *Direcția Generală de Politici şi Strategii CDI şi Digitalizare.*

Directoratul Național de Securitate Cibernetică (DNSC) – este autoritatea competentă la nivel național pentru *securitatea rețelelor şi sistemelor informatice* care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale.

Conform art. 15 alin.2 din Legea NIS, pentru asigurarea unui nivel ridicat de securitate a rețelelor şi sistemelor informatice, DNSC se consultă şi cooperează cu:

„a) *Serviciul Român de Informații*, pentru securitatea rețelelor şi a sistemelor informatice care asigură servicii esențiale a căror afectare aduc atingere securității naționale;

b) *Ministerul Apărării Naționale*, pentru securitatea rețelelor şi a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea națională;

c) *Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale şi Serviciul de Protecție şi Pază*, pentru securitatea rețelelor şi a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate şi responsabilitate".

De asemenea, conform art.16 din aceeaşi lege, DNSC se consultă şi cooperează, după caz, cu:

„a) *organele de urmărire penală;*

b) *Autoritatea Națională pentru Administrare şi Reglementare în Comunicații*, atunci când incidentele au ca rezultat afectarea securității ori funcționării rețelelor publice de comunicații electronice ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate şi responsabilitate a acesteia;

c) *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii".

Concluzii

Extinderea digitalizării a impus un nou tip de audit - auditul sistemelor informatice - care constă în evaluarea dezvoltării, întreținerii, funcționării, securității şi controlului sistemelor informatice.

Într-o economie globală, din ce în ce mai digitalizată, în care informatizarea a pătruns şi în domenii de interes public precum învățământ, sănătate, administrație publică, justiție, diplomație, importanța auditului sistemelor informatice a crescut continuu ca urmare a aptitudinii acestuia de a identifica vulnerabilitățile şi riscurile care privesc utilizarea sistemelor informatice.

Eşecul în asigurarea securității sistemelor informatice şi scandalurile în care au fost implicate companii, dar şi instituții publice, oameni de afaceri, oameni politici şi ziarişti, au determinat o schimbare de viziune în privința rolului auditului, dar şi în abordarea acestuia, fiind promovată orientarea spre risc. Analiza riscurilor permite identificarea vulnerabilităților sistemului informatic astfel încât auditorul să poată determina controalele necesare pentru a minimiza aceste riscuri. Auditul sistemelor informatice contribuie la creşterea încrederii în activitatea desfăşurată cu utilizarea acestor sisteme, prin asigurarea unui nivel superior de securitate a datelor stocate de acestea.

Bibliografie

1. M. Boulescu, M. Ghiță, V. Mareş, *Fundamentele auditului*, Ed. Didactică şi Pedagogică, Bucureşti, 2001;

2. I. F. Chiş, L. S. Tudor, *Auditul sistemelor informatice*, în Conferința Academia Comercială Satu Mare 2014;

3. http://conferinta.academiacomerciala.ro/CD2014/articole/2/AUDITUL%20SISTEMELOR%20INFORMATICE%20Chis%20Todor.pdf;

4. Massimo Ciambotti, *Luca Pacioli, la Partita Doppia e la storia della contabilità e della società,* Centro Studi Mario Pancrazi, https://www.centrostudimariopancrazi.it/images/pubblicazioni/before_and_after_luca_pacioli/9.pdf;

5. I. Ivan, A. Felician, S. Capisizu, *Auditul informatic*, în Economistul, 1887/2005, http://alecu.ase.ro/articles/economistul_2005.pdf;

6. V. Kumar, *Auditing. Basic concepts of auditing,* https://prgc.ac.in/uploads/study_material/5th%20sem%20I%20Unit%20Auditing%20PPT-1.pdf334.pdf;

7. P. Năstase (coordonator) ş.a., *Auditul şi controlul sistemelor informaționale*, Ed. Economică, Bucureşti, 2007;

8. D. D. Şaguna, D. Şova, *Drept financiar public*, Ed. All Beck, Bucureşti, 2005.