Article

Codul etic al auditorului de securitate cibernetică. Reglementări interne și internaționale

(Cyber Security Auditor Code of Ethics. National and International Regulations)

Ramona CIOBANU[1]*

[1] Universitatea Transilvania din Brașov,
* Correspondent: ramona.ciobanu@unitbv.ro

Rezumat: *Extinderea implementării sistemelor informatice a determinat apariția unui nou tip de audit, auditul cibernetic, și a unei noi profesii liberale, auditorul de securitate cibernetică. Asociațiile profesionale nou create, organizațiile internaționale și statele au adoptat norme care privesc, pe de o parte, desfășurarea auditului cibernetic și, pe de altă parte, Coduri etice ca ansamblu de norme, principii și valori care guvernează activitatea auditorilor de securitate cibernetică.*

Cuvinte cheie: *audit, audit cibernetic, auditor de securitate cibernetică, Cod etic*

Abstract: *The expansion of the implementation of information systems has led to the emergence of a new type of audit, cyber audit, and a new liberal profession, the cybersecurity auditor. Newly created professional associations, international organizations and states have adopted the rules governing, on the one hand, the conduct of cyber audit and, on the other hand, the Codes of Ethics as a set of norms, principles and values that govern the work of cybersecurity auditors.*

Keywords: *audit, cyber audit, cybersecurity auditor, Codes of Ethics*

Citation: Ciobanu, R. (2022). Codul etic al auditorului de securitate cibernetică. Reglementări interne și internaționale. *Etică și Deontologie. 2*(1), 48-60
https://doi.org/10.52744/RED.2022.01.06

Publisher's Note: RED stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Profesia de auditor de securitate cibernetică

Desfășurarea activității economice, dar și a operațiunilor cu bani publici, au impus încă din cele mai vechi timpuri necesitatea ținerii evidenței veniturilor și cheltuielilor, a controlului corectitudinii, veridicității și legalității acestor înregistrări și, pe o anumită treaptă de dezvoltare a societății, a auditului financiar ca formă superioară de analiză, sinteză și orientare care are ca scop verificarea corectitudinii, legalității, eficienței și eficacității operațiunilor financiare efectuate în cadrul unei instituții. Auditul financiar este o activitate caracterizată prin independență și obiectivitate, menită să dea asigurări și consiliere conducerii instituției auditate privind administrarea veniturilor, având aptitudinea de a contribui la creșterea eficienței acestei instituții printr-o abordare bazată pe gestiunea riscului (Șaguna, Șova, 2005).

Dacă inițial noțiunea de audit a fost asociată cu auditul financiar, sensul larg al noțiunii incluzând și auditul contabil, precum și pe cel fiscal, astăzi activitatea de audit s-a extins și asupra altor domenii, precum protecția mediului, capitalul intelectual, sistemele informatice (Ciobanu, 2022a).

Extinderea implementării sistemelor informatice în cele mai diverse activități umane și-a pus amprenta asupra activității de audit care a început să utilizeze tehnicile automate de audit datorită avantajelor pe care le presupun acestea: economie de timp și de resurse financiare, rapiditate, acuratețe, precizie (Dhillon, 2000). Pe de altă parte, folosirea sistemelor informatice prezintă pe lângă avantaje și riscuri specifice (Kassa, 2016) astfel încât s-a simțit nevoia implementării unor tehnici de control al sistemelor informatice pentru identificarea vulnerabilităților acestora. Chiar dacă de obicei se pleacă de la premisa că informațiile generate de calculator sunt corecte, auditorii financiari, oameni ai cifrelor, dar și experți în efectuarea de analize și conexiuni, și-au dat seama că folosirea sistemelor informatice impune verificarea integrității datelor, aceasta devenind o etapă premergătoare îndeplinirii obiectivelor misiunii lor de audit, astfel încât rezultatele din rapoartele de audit să fie bazate pe date complete și precise. Procedurile de control și certificare a datelor s-au născut din nevoia de încredere (Ciobanu, 2022a).

Institutul American al Contabililor Autorizați (American Institute of Certified Public Accountants – AICPA) a lansat în anul 1968 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 și-a propus să elaboreze standarde, ghiduri și proceduri pentru noul tip de audit. Constituirea acestei asociații profesionale marca așadar apariția unui nou tip de audit, auditul sistemelor informatice sau auditul cibernetic, cum mai este astăzi numit, ca

audit de sine-stătător, cu reguli şi obiective specifice, desprinzându-se de auditul financiar cu care a fost asociat iniţial.

În 1994, EDPAA îşi schimbă denumirea în Information Systems Audit and Control Association (Asociaţia pentru Auditul şi Controlul Sistemelor Informaţionale), cunoscută sub acronimul ISACA, asociaţie care prin activitatea desfăşurată s-a impus pe plan internaţional ca leader în certificare, dar şi în asigurarea instrumentelor de lucru pentru activitatea de audit al sistemelor informatice prin adoptarea de standarde, ghiduri, proceduri specifice, aşa-numitul cadru de lucru COBIT (Control Objectives for Information and related Technology), folosit de auditorii de securitate informatică atât în auditul privat, cât şi în cel public. COBIT a fost armonizat cu o serie de standarde şi bune practici IT şi acţionează în prezent ca un integrator al acestor standarde, sintetizând obiectivele principale sub un singur cadru de referinţă general acceptat (Ciobanu, 2022b).

Literatura de specialitate defineşte auditul sistemelor informatice drept „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 capacităţii sistemului informatic de a atinge obiectivele strategice ale unei organizaţii, utilizând eficient resursele informaţionale şi asigurând integritatea datelor prelucrate şi stocate" (Năstase ş.a., 2007).

Această activitate complexă este desfăşurată de auditorul sistemelor informatice sau auditorul cibernetic, specialist în domeniul controlului, securităţii şi managementului sistemelor informatice, atestat să desfăşoare această activitate.

Auditul sistemelor informatice poate fi realizat de auditori angajaţi ai instituţiei auditate, ca audit intern, sau de auditori independenţi, persoane fizice sau juridice, ca urmare a încheierii contractului de audit cu instituţia auditată, ca audit extern. Auditul intern verifică respectarea procedurilor de transformare a datelor de intrare în rezultate, urmărindu-se modul în care sistemul care se implementează este mai eficient, fiind însoţit de o economisire a resurselor, iar auditul extern testează procedurile de control care intră în componenţa sistemului, proceduri care implementează exigenţele cuprinse în specificaţii, standarde, acte normative şi care restricţionează prin blocare orice tentativă de execuţie a operaţiunilor interzise (Ivan, Felician, Capisizu, 2005).

Auditorii de securitate informatică au următoarele obiective (Năstase ş.a., 2007):

- identificarea şi evaluarea riscurilor de sistem,
- verificarea funcţiilor incompatibile în cadrul sistemului informatic,
- verificarea securităţii fizice şi logice a sistemului informatic,
- verificarea şi evaluarea infrastructurii reţelelor de calculatoare,
- controlul aplicaţiilor informatice,

- testarea integrității datelor,
- verificarea existenței și securității copiilor de siguranță a datelor, informațiilor, aplicațiilor informatice,
- -verificarea și evaluarea planurilor de recuperare în caz de dezastre.

Din rațiuni de identitate cu terminologia folosită de legislația din România, dar și cu cea folosită de normele Uniunii Europene, voi folosi în continuare termenii de audit cibernetic și auditor de securitate cibernetică.

2. Deontologia profesiei de auditor de securitate cibernetică. Coduri etice adoptate în cadrul asociațiilor profesionale pe plan internațional. Principii diriguitoare.

Etimologic, noțiunea de deontologie provine din limba franceză, de la cuvântul déontologie, și poate fi definită ca fiind teoria datoriei, a obligațiilor morale. Deontologia reprezintă totalitatea normelor de conduită și a obligațiilor etice ale unei profesii.

Deontologia auditului presupune elaborarea unui cod etic pentru auditori, cod prin care să se stabilească valorile și principiile care trebuie să călăuzească activitatea de audit. Adoptarea și aplicarea unui cod etic pentru auditori este de natură să promoveze încrederea în auditori și în activitatea lor, respectul, siguranța și credibilitatea acestora. Nevoia de credibilitate impune ca opiniile auditorilor să fie considerate exacte și de încredere de către utilizatorii rapoartelor de audit: entitatea auditată, clienții și partenerii de afaceri ai acesteia, instituțiile statului, opinia publică. În general, auditorul favorizează o asemenea atitudine prin integritate, independență, obiectivitate, neutralitate politică, evitarea conflictelor de interese, confidențialitate, competență și pregătire profesională.

Întrucât activitatea de audit a demarat ca audit contabil, financiar și fiscal, de-a lungul timpului au fost adoptate coduri etice în cadrul diferitelor asociații profesionale ale contabililor și auditorilor financiari, valorile și principiile acestora fiind preluate și incluse în norme juridice aplicabile auditorilor din sectorul public. În acest sens putem da exemplul codurilor etice adoptate în cadrul:

- IFAC - International Federation of Accountants accesibil la adresa:
  - https://www.ifac.org/system/files/publications/files/Code-of-Ethics _July_2009_FINAL_02_23_10.pdf),
  - -The IIA – The Institute of Internal Auditors accesibil la adresa: https://www.theiia.org/en/standards/what-are-the-standards/ mandatory-guidance/code-of-ethics/
- INTOSAI - International Organization of Supreme Audit Institutions accesibil la adresa: https://www.issai.org/wp-content/uploads/2019/08/ISSAI-130-Code-of-Ethics.pdf

- SAIs - European Union's Supreme Audit Institutions accesibil la adresa: https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf

Din aceste documente rezultă un set de valori, acceptate unanim ca principii nucleu, fundamentale (core principles), cu rol diriguitor în activitatea de audit, după cum urmează:

- independenţă,
- integritate,
- obiectivitate,
- competenţă,
- profesionalism,
- confidenţialitate.

În ceea ce priveşte auditul cibernetic, în cadrul ISACA (Information Systems Audit and Control Association), după constituirea organizaţiei, un prim demers a fost acela de a elabora Codul de etică profesională, cod care valorifică principiile fundamentale ale activităţii de audit şi care cuprinde un set de reguli de comportament ce ghidează conduita etică şi profesională a auditorilor sistemelor informatice certificaţi. Astfel, exercitarea acestei profesii trebuie să se supună următoarelor principii (Năstase ş. a., 2007; Ciobanu, 2022b):

- implementarea standardelor şi procedurilor specifice de audit SI,
- seriozitate şi loialitate faţă de client,
- abţinere de la activităţi ilegale,
- confidenţialitatea informaţiilor obţinute în timpul misiunii de audit, cu excepţia situaţiei în care acestea sunt solicitate de autorităţi legale,
- independenţa auditorului ca premisă a corectitudinii şi lipsei de prejudecăţi,
- profesionalism,
- informarea clientului cu privire la rezultatele auditului,
- susţinerea informării asociaţilor/acţionarilor/membrilor entităţii auditate pentru a creşte gradul de înţelegere a aspectelor referitoare la securitatea şi controlul sistemelor informatice, precum şi a încrederii în cadrul grupului.

3. Reglementarea profesiei de securitate cibernetică în România

Schimbările intervenite în economia mondială ca urmare a implementării sistemelor informatice şi a noilor reţele de comunicaţii, precum şi nevoia de interconectare a economiilor naţionale ale statelor au determinat adoptarea unor noi acte normative şi în România, corespunzătoare noilor realităţi, precum: Legea nr. 455/2001 privind semnătura electronică, Legea nr. 365/2002 privind comerţul

electronic, Legea nr. 506/2004 privind protecția datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, Legea nr. 64/2004 pentru ratificarea Convenției privind criminalitatea informatică adoptată în cadrul Consiliului Europei.

De asemenea, ca o reflectare a preocupării existente pe plan internațional, dar și în cadrul Uniunii Europene, privind asigurarea securității sistemelor informatice, ca o condiție a bunei desfășurări a activităților care utilizează aceste sisteme, în România au fost adoptate:

- H.G. nr. 271/2013 pentru aprobarea Strategiei de Securitate Cibernetică a României (SNSC) și a Planului de acțiune la nivel național privind implementarea SNSC,
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice denumită și Legea NIS și care transpune în legislația internă Directiva UE 2016/1148 (NIS – Network and Information Security) a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în UE,
- O.U.G. nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.

În mod firesc, odată cu extinderea implementării sistemelor informatice în România, dar și ca urmare a adoptării unui cadru legislativ adecvat, s-a simțit nevoia de auditare a sistemelor informatice ca o garanție a securității mediului informatizat, astfel încât a apărut o nouă profesie liberală: cea de auditor de securitate cibernetică. Pentru reglementarea exercitării acesteia a fost adoptat Ordinul nr. 559/2021 al Secretarului General al Guvernului privind aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică, pentru care voi folosi în continuare denumirea de Regulament, act normativ care reglementează atestarea, suspendarea și revocarea atestatului de auditor de securitate cibernetică, desfășurarea activității auditorilor și a misiunii de audit, verificarea activității auditorilor de securitate cibernetică și aplicarea sancțiunilor, evidența auditorilor prin Registrul Național al Auditorilor de Securitate Cibernetică. Potrivit art. 1 alin. 1, Regulamentul se aplică auditorilor de securitate cibernetică pentru auditarea rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale în condițiile Legii NIS.

Regulamentul definește auditorul de securitate cibernetică drept „persoană fizică atestată sau persoană juridică cu personal atestat care realizează activități de auditare a rețelelor și sistemelor informatice ce susțin servicii esențiale sau furnizează servicii digitale, conform reglementărilor și bunelor practici în domeniu” (art. 2 alin. 2 lit. a). Un serviciu este considerat esențial dacă furnizarea lui îndeplinește cumulativ următoarele condiții (art. 6 alin. 1 din Legea NIS): (1) serviciul este esențial în susținerea unor activități societale și/sau economice de cea mai mare

importanță; (2) furnizarea sa depinde de o rețea sau de un sistem informatic; (3) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident. In concreto, sunt servicii esențiale cele din energie, transport, sectorul bancar și piața financiară, domeniul medical, infrastructură digitală, furnizarea și distribuirea apei potabile. Furnizorul de servicii digitale este orice entitate care furnizează servicii care se încadrează într-una din următoarele categorii: piață online, motor de căutare online, serviciu de cloud computing (art. 3 lit. o din Legea NIS).

Regulamentul definește auditul de securitate cibernetică ca fiind „activitatea prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul rețelelor și sistemelor informatice în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora" (art. 2 alin. 2 lit. b), constituind „unul dintre mijloacele disponibile oricărui operator economic pentru a testa și asigura nivelul de securitate al rețelelor și sistemelor informatice care stau la baza susținerii serviciilor esențiale sau furnizării de servicii digitale" (art. 27 alin. 1).

DECLARAȚIE/ANGAJAMENT

privind respectarea Codului etic al auditorului de securitate cibernetică

Auditor de securitate cibernetică: ..... IDASC: .....

Subsemnatul, ... (nume și prenume), atestat ca auditor de securitate cibernetică având IDASC: ....., posesor al actului de identitate seria ..... nr....., CNP....., cunoscând dispozițiile art. 326 din Codul penal cu privire la falsul în declarații, declar pe propria răspundere că am luat cunoștință de Codul etic al auditorului de securitate cibernetică și mă angajez să îl respect pe întreg parcursul perioadei de valabilitate a atestatului de securitate cibernetică. Dau prezenta declarație în conformitate cu art. 20 din Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021, fiindu-mi necesară la CERT-RO/ANSRSI pentru înscrierea ca auditor de securitate cibernetică în Registrul național al auditorilor de securitate cibernetică. Semnătura auditorului de securitate cibernetică.

Numele și prenumele semnatarului .....

Data .....

Figura 1. Model de declarație/angajament privind respectarea Codului etic al auditorului de securitate cibernetică

Sursa: Art. 12 din Anexa 13 – *Codul Etic al auditorului de securitate cibernetică* - a Ordinului nr. 559/2021 al Secretarului General al Guvernului privind aprobarea Regulamentului *pentru atestarea și verificarea auditorilor de securitate cibernetică*

În Anexa nr. 13 a Regulamentului este reglementat Codul Etic al auditorului de securitate cibernetică, Cod la respectarea căruia sunt obligați toți auditorii atestați să exercite această profesie, potrivit art. 20 alin. 1 din Regulament. După obținerea atestatului de auditor de securitate cibernetică, auditorul este obligat să semneze, olograf sau digital, declarația/angajamentul privind respectarea Codului etic al auditorului de securitate cibernetică (Figura 1) și o/îl va înainta autorității competente la nivel național, actualmente Directoratul Național de Securitate Cibernetică (fostul CERT-RO), în maximum 10 zile de la emiterea atestatului (art. 20 alin. 2 din Regulament). Nesemnarea și/sau netransmiterea declarației/angajamentului duce la suspendarea sau la revocarea atestatului, după caz (art. 20 alin. 3 din Regulament).

4. Codul etic al auditorului de securitate cibernetică din România

Potrivit art. 1 din Codul etic al auditorului de securitate cibernetică, pe care-l voi numi în continuare Codul etic, acesta „reprezintă un ansamblu de principii și reguli de conduită care trebuie să guverneze activitatea auditorului de securitate cibernetică", scopul lui fiind, potrivit art. 3, acela de a asigura „cadrul etic necesar desfășurării activității de auditor de securitate cibernetică, astfel încât acesta să își îndeplinească cu profesionalism, loialitate, corectitudine și în mod imparțial îndatoririle de serviciu și să se abțină de la orice faptă care ar putea să aducă prejudicii" entității auditate.

Codul etic reglementează în două capitole distincte (Capitolele II și III) principiile și regulile de conduită aplicabile exercitării acestei profesii.

4.1. Principii

Principiile enunțate în Codul etic valorifică principiile consacrate pe plan internațional în Codurile etice ale auditorilor, acele core principles, principii nucleu, unanim recunoscute ca fiind esențiale pentru atingerea obiectivelor misiunii de audit.

Astfel, potrivit art. 6 din Codul etic, în desfășurarea misiunii de audit, auditorul de securitate cibernetică este obligat să respecte următoarele principii fundamentale: integritate, independență și obiectivitate, confidențialitate, competență profesională și neutralitate politică.

Principiul integrității este reglementat după cum urmează (art. 6 alin. 1 lit. a din Codul etic): „integritatea - auditorul de securitate cibernetică trebuie să fie corect, onest și incoruptibil, integritatea fiind suportul încrederii și credibilității acordate raționamentului auditorului de securitate cibernetică".

Pentru explicarea conținutului acestui principiu, Codul etic adoptat în cadrul IFAC, revizuit în anul 2009, prevede la Secțiunea 110 intitulată „Integritatea" că integritatea impune tuturor auditorilor obligația de a avea un comportament sincer, onest, de a nu fi asociat cu declarații, comunicări, rapoarte care conțin informații înșelătoare, false, care induc în eroare (IFAC, 2009).

De asemenea, Codul etic ISSAI 130, adoptat în cadrul INTOSAI în anul 2019, identifică următoarele vulnerabilități pentru integritate (INTOSAI, 2019):

- interese personale sau financiare,
- cadouri, gratuități,
- implicarea în activități politice, grupuri de presiune sau de lobby,
- acces la informații sensibile sau confidențiale,
- circumstanțe legate de viața personală a auditorului cum ar fi situația, financiară sau relațiile personale.

Totodată Codul etic ISSAI 130 atrage atenția că respectarea reglementărilor specifice activității de audit nu reprezintă un proces formal, ci trebuie să se ia în

considerare scopul pentru care au fost adoptate şi că pentru apărarea principiului integrităţii ar trebui luate măsuri precum existenţa unui organism/a unor consilieri de etică la care să fie raportate suspiciunile de încălcare a integrităţii, dar şi organizarea unor întâlniri, conferinţe, workshop-uri care să promoveze cultura integrităţii şi să dezbată riscuri specifice cu caracter de noutate (INTOSAI, 2019).

Principiile independenţei şi obiectivităţii sunt reglementate după cum urmează (art. 6 alin. 1 lit. b din Codul etic):

a) „independenţa şi obiectivitatea:
   - *independenţa* - independenţa faţă de operatorul economic (operator de servicii esenţiale sau furnizor de servicii digitale) şi oricare alte grupuri de interese este indispensabilă. În acest sens, auditorul de securitate cibernetică trebuie:
     - să depună toate eforturile pentru a fi independent în tratarea problemelor aflate în analiză;
     - să fie independent şi imparţial atât în teorie, cât şi în practică;
     - să nu fie afectat de interese personale sau exterioare;
     - să nu se implice în acele activităţi în care are un interes legitim/ întemeiat;
   - *obiectivitatea* - în activitatea sa auditorul de securitate cibernetică trebuie:
     - să manifeste obiectivitate şi imparţialitate în redactarea rapoartelor, care trebuie să fie precise şi obiective;
     - să formuleze concluzii şi opinii bazate exclusiv pe documentele obţinute şi analizate conform listei standardelor şi specificaţiilor internaţionale şi europene în domeniu;
     - să folosească toate informaţiile utile primite de la operatorul economic auditat şi din alte surse;
     - să analizeze punctele de vedere exprimate de operatorul economic auditat şi, în funcţie de pertinenţa acestora, să formuleze opiniile şi recomandările proprii;
     - să facă o evaluare echilibrată a tuturor circumstanţelor relevante şi să nu fie influenţat de propriile interese sau de interesele altora în formarea propriei opinii".

Codul etic IFAC prevede la Secţiunea 290 că independenţa are două aspecte (IFAC, 2009):

b) independenţa raţionamentului care constă în efectuarea misiunii de audit cu obiectivitate şi scepticism profesional, precum şi formularea de concluzii în afara oricăror influenţe;
c) independenţă în atitudine care constă în evitarea oricăror fapte sau circumstanţe care pot pune la îndoială integritatea şi obiectivitatea auditorului.

Totodată, din Codul etic ISSAI 130 (INTOSAI, 2019) rezultă că independența privește statutul auditorului, mandatul acestuia, efectuarea auditului, raportarea, precum și raportul cu managementul entității auditate, putând constitui garanții ale independenței auditorului următoarele:

- independența față de influența politică,
- independență față de managementul entității auditate,
- neauditarea propriei activități,
- evitarea auditării entităților în care au avut recent calitatea de salariați,
- evitarea situațiilor în care situația personală i-ar putea afecta obiectivitatea,
- refuzul cadourilor, gratuităților, tratamentului preferențial/privilegiat.

În ceea ce privește obiectivitatea, Codul etic IFAC prevede la secțiunea 120 intitulată „Obiectivitate" (IFAC, 2009) că auditorul nu trebuie să accepte o misiune de audit dacă o relație sau o circumstanță i-ar putea afecta raționamentul profesional, obiectivitatea presupunând imparțialitate, nepărtinire, ferire de influențe.

Principiul confidențialității este reglementat după cum urmează (art. 6 alin. 1 lit. c din Codul etic):

- *confidențialitatea*:
  - auditorul de securitate cibernetică este obligat:
    - să păstreze confidențialitatea în legătură cu faptele, informațiile sau documentele despre care ia cunoștință în exercitarea atribuțiilor lor; este interzis să utilizeze în interes personal sau în beneficiul unui terț informațiile dobândite în exercitarea atribuțiilor de serviciu;
    - să protejeze informațiile referitoare la auditul de securitate și, în special, dovezile, constatările și rapoartele;
- în cazuri excepționale auditorul de securitate cibernetică poate furniza aceste informații numai în condițiile expres prevăzute de normele legale în vigoare sau cu autorizația scrisă din partea operatorului economic auditat".

Codul etic IFAC prevede la secțiunea 140 intitulată „Confidențialitate" (IFAC, 2009) că este interzisă dezvăluirea informațiilor confidențiale fără drept sau fără să existe o obligație legală în acest sens, precum și folosirea acestora în interes personal sau al unor terți.

Principiul competenței profesionale este reglementat după cum urmează (art. 6 alin. 1 lit. d din Codul etic):

- *competența profesională*:
  - auditorul de securitate cibernetică este obligat să își îndeplinească atribuțiile pe timpul activității de audit de securitate cu profesionalism, competență, imparțialitate și la standarde internaționale, aplicând cunoștințele, aptitudinile și experiența dobândite;

- auditorul de securitate cibernetică este obligat să respecte legile și reglementările naționale aplicabile, precum și cele mai bune practici legate de activitățile de audit de securitate".

Codul etic IFAC prevede la secțiunea 130 intitulată „Competență profesională și diligență" (IFAC, 2009) că principiul competenței profesionale impune următoarele obligații:

- menținerea competenței profesionale la nivelul necesar pentru a se asigura că angajatorii sau clienții beneficiază de servicii profesionale și competente,
- desfășurarea activității cu diligență, în conformitate cu standardele, pentru furnizarea de servicii profesionale,
- serviciile profesionale competente presupun un bun raționament profesional în aplicarea cunoștințelor și aptitudinilor profesionale.

Competența profesională presupune două etape: (1) dobândirea și (2) menținerea acesteia prin formare continuă, iar diligența se referă la obligația de a acționa în conformitate cu cerințele misiunii, cu atenție, cu temeinicie și în timp util. Totodată, profesionistul trebuie să aducă la cunoștința beneficiarilor Raportului de audit întocmit la finalul misiunii de audit limitele inerente ale activităților desfășurate (IFAC, 2009). Aceasta este explicația faptului că în Raportul de audit auditorul inserează un paragraf în care precizează că din cauza limitelor inerente controalelor interne, frauda și erorile pot să apară sau să rămână nedetectate și un alt paragraf în care precizează că auditul nu poate detecta toate punctele slabe din cadrul procedurilor de control atâta timp cât auditul nu este o activitate continuă, iar testarea procedurilor de control de către auditor se realizează prin sondaj. Este o modalitate prin care avertizează utilizatorul raportului cu privire la limitele inerente, dar și o modalitate de a se pune la adăpost de eventualele acuzații care i s-ar putea aduce.

Principiul neutralității politice este reglementat după cum urmează (art. 6 alin. 1 lit. e din Codul etic):

- *neutralitatea politică*:
  - auditorul de securitate cibernetică trebuie să fie neutru din punct de vedere politic, în scopul îndeplinirii în mod imparțial a activităților; în acest sens el trebuie să își mențină independența față de orice influențe politice;
  - auditorul de securitate cibernetică are obligația ca în exercitarea atribuțiilor ce îi revin să se abțină de la exprimarea sau manifestarea convingerilor lui politice".

4.2. Reguli de conduită

În accepțiunea Codului etic, regulile de conduită sunt norme de comportament adresate auditorului de securitate cibernetică și reprezintă un instrument „pentru interpretarea principiilor și aplicarea lor practică" (art. 7 din Codul etic), având rolul

să-l îndrume pe acesta din punct de vedere etic. Capitolul III din Codul etic intitulat Reguli de conduită reia principiile enunțate la articolul 6 și aduce lămuriri privitoare la conținutul acestora, completând interpretarea lor legală.

Astfel, integritatea presupune exercitarea profesiei cu onestitate, bună-credință și responsabilitate; respectarea legii și bunelor practici în materie de audit cibernetic; respectarea obiectivelor etice legitime ale instituției din care provine; interzicerea de a participa cu bună știință la activități ilegale și angajamente care discreditează îndeplinirea atribuțiilor de auditor de securitate cibernetică sau instituția din care face parte.

Independența și obiectivitatea auditorului presupun: evitarea conflictului de interese; menținerea în limitele competențelor specifice activității de audit al securității cibernetice; abținerea de la activități care i-ar putea afecta obiectivitatea; onestitate în raport cu entitatea auditată.

Confidențialitatea presupune păstrarea secretului informațiilor obținute în cursul activității de audit de securitate, interzicerea folosirii acestora în scop personal, în mod ilegal sau în detrimentul obiectivelor legitime și etice ale entității auditate.

Competența de care trebuie să dea dovadă auditorul implică comportament profesionist; aplicarea standardelor, normelor, procedurilor, ghidurilor și bunelor practici de audit; imparțialitate în îndeplinirea atribuțiilor specifice; acceptarea misiunilor de audit pentru care are cunoștințele, aptitudinile și experiența necesare; formare continuă; auditorii persoane juridice să asigure condițiile necesare pregătirii profesionale a auditorilor de securitate cibernetică; cunoașterea legislației aplicabile activității de audit, dar și a celei care reglementează activitatea entității auditate; auditorul de securitate cibernetică nu trebuie să depășească atribuțiile specifice profesiei.

Directoratul Național de securitate cibernetică prin Autoritatea Națională pentru Securitatea Rețelelor și Sistemelor Informatice (ANSRSI) verifică respectarea prevederilor Codului etic de către auditorii de securitate cibernetică, persoane fizice și persoane juridice, și poate aplica sancțiuni care pot culmina cu revocarea atestatului de auditor de securitate cibernetică.

5. Concluzii

Existența unor norme etice privitoare la exercitarea profesiei de auditor de securitate cibernetică, dar și a unor instituții cu atribuții de supraveghere a respectării acestora sunt măsuri menite să asigure încrederea în activitatea acestor specialiști, să le sporească prestigiul profesional. Supravegherea moralității desfășurării activității de auditor de securitate cibernetică nu trebuie percepută de auditor ca o presiune exercitată asupra lui, ci ca pe un ajutor cu important rol corectiv

și de asigurare a performanței în activitatea desfășurată (Raval, 2015). Totodată, un audit cibernetic de calitate presupune înțelegerea implicațiilor etice ale sistemelor informatice auditate (Cooke, 2020).

Referințe:

Ciobanu, R. (2022a), Tendințe actuale în activitatea de audit. Auditul sistemelor informatice, în *Revista Universul Juridic* nr. 2/2022.

Ciobanu, R. (2022b), Rolul organizațiilor internaționale în elaborarea standardelor de audit al securității cibernetice, în *Revista Universul Juridic* nr. 3/2022.

Cooke, I. (2020), IS Audit Basics: Ethics in Information Technology: *ISACA Journal*, Volume 6, 2020, https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/ethics-in-information-technology

Dhillon, G. (2000), *Interpreting key issues in IS/IT benefits management*, Proceedings of the 33rd Hawaii Intenational Conference on System Sciences 2000, https://www.researchgate.net/publication/221180043_Interpreting_Key_Issues_in_ISIT_Benefits_Management

IIA, Code of Ethics, https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/code-of-ethics/

IFAC, Interntional Ethics Standards Board for Accountants (2009), Code of Ethics for Professional Accountants, https://www.ifac.org/system/files/publications/files/Code-of-Ethics_July_2009_FINAL_02_23_10.pdf

INTOSAI (2019), ISSAI 130 Code of Ethics, https://www.issai.org/wp-content/uploads/2019/08/ISSAI-130-Code-of-Ethics.pdf

ISACA, Code of Professional Ethics, https://www.isaca.org/credentialing/code-of-professional-ethics

Ivan, I., Felician, A., Capisizu, S., (2005) Auditul informatic, în *Economistul* 1887/2005, 18, http://alecu.ase.ro/articles/economistul_2005.pdf

Kassa, S.G. (2016), Information Systems Security Audit. An Ontological Framework: *ISACA Journal*, Volume 5, 2016, https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/information-systems-security-audit-an-ontological-framework

Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice (Legea NIS).

Năstase, P. (coordinator), ș.a. (2007), *Auditul și controlul sistemelor informaționale*, București, Editura Economică, București, 2007, 14, 16-18.

Ordinul nr. 559/2021 al Secretarului General al Guvernului privind aprobarea Regulamentului din 22 martie 2021 privind atestarea și verificarea auditorilor de securitate cibernetică.

Raval, V. (2015), Monitoring Morality. Is Assurance of Information Etics Feasible?: *ISACA Journal*, Volume 5, 2015, https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/information-ethics-monitoring-moralityis-assurance-of-information-ethics-feasible

SAIs, Contact Committee (2020), Audit Compendium, Cybersecurity in the EU and its Member States. Auditing the rezilience of critical information systems and digital infrastructures to cyber attacks. upreme audit institution reports relating to cybersecurity 2014 and 2020, https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf