Revista Universul Juridic ● nr. 3, martie 2022, pp. 134-148

ROLUL ORGANIZAȚIILOR INTERNAȚIONALE ÎN ELABORAREA STANDARDELOR DE AUDIT AL SECURITĂȚII CIBERNETICE

Ramona CIOBANU
Facultatea de Drept
Universitatea „Transilvania" din Braşov

Abstract

Given the potential negative impact of cyber threats on economy, social peace, political stability and even democracy itself, taking action to increase cybersecurity is an imperative requirement at the governmental level, but also at the level of each entity operating with information systems. Key tools in this regard are both cybersecurity standards and cybersecurity audit standards, in the adoption and implementation of which an important role is played by international organizations. These standards ensure increased performance, security and economic growth.

Keywords: *cybersecurity, auditing, standards, international organizations.*

1. Standardele de securitate cibernetică şi Standardele de audit al securității cibernetice

Având în vedere complexitatea sistemelor informatice, legătura acestora cu eficiența şi deci cu succesul entității utilizatoare, anticipând extinderea utilizării sistemelor informatice şi prejudiciile care ar putea fi produse de carențele în exploatarea acestora, de timpuriu s-a pus problema necesității unor standarde, atât pentru securitatea cibernetică, cât şi pentru auditul securității cibernetice.

Cybersecurity sau securitatea cibernetică se referă la activitățile necesare pentru a proteja sistemele informaționale, utilizatorii acestora şi alte persoane afectate de amenințările cibernetice şi implică prevenirea, detectarea, răspunsul şi recuperarea în urma incidentelor cibernetice. Aceste incidente pot fi intenționate sau neintenționate şi pot consta în dezvăluirea accidentală de informații, atacuri cibernetice (Malware, Ransomware, Distributed Denial-of-Service, Web-based Attacks, Social Engineering, Cyberspionage), furt de date şi chiar imixtiune în procesele

democratice, precum interferențe în procesele electorale şi campanii de dezinformare[1]. Având în vedere potențialul impact negativ al acestor activități asupra economiei, păcii sociale, stabilității politice şi chiar asupra democrației însăşi, adoptarea unor măsuri menite să crească nivelul securității cibernetice reprezintă o cerință imperios necesară la nivel guvernamental, dar şi la nivelul fiecărei entități care operează cu sisteme informatice.

Instrumente cheie în acest sens sunt *standardele de securitate cibernetică* prin a căror aplicare, instituția se asigură că strategia şi politicile sale sunt implementate eficient. Implementarea standardelor de securitate cibernetică presupune costuri, dar acestea sunt infinit mai mici în comparație cu prejudiciile pe care le poate provoca un incident de securitate cibernetică. Cu cât datele, numărul partenerilor şi amplitudinea activității sunt mai mari, cu atât mai mare este şi nevoia de implementare a unor măsuri de sporire a securității sistemelor informaționale. Cu toate acestea, standardele de securitate cibernetică odată implementate nu sunt o garanție infailibilă pentru securitatea cibernetică. Trebuie realizată o supraveghere continuă a succesului implementării, a conformării la standarde, în caz contrar eficiența lor poate fi erodată în timp. Standardele implementate într-o instituție sunt adesea sintetizate într-o matrice care constituie oglinda standardelor utilizate şi a controalelor asociate acestora, având un rol important pentru managementul securității sistemelor informatice şi pentru activitatea de audit al securității cibernetice[2].

Standardele de securitate cibernetică reprezintă un instrument de gestionare şi limitare a riscului la un nivel acceptabil şi trebuie să fie în concordanță cu guvernanța IT a instituției – cu activitatea de conducere şi coordonare a activității IT din instituția respectivă şi cu strategia de securitate cibernetică[3]. Am putea defini standardele de securitate cibernetică un set de bune practici care au ca scop protecție în fața amenințărilor cibernetice şi creşterea gradului de securitate cibernetică.

Din rapoartele instituțiilor supreme de audit ale statelor membre ale UE rezultă că, până în anul 2018, jumătate dintre acestea nu au efectuat un audit al securității sistemelor informatice, fapt care a determinat preocuparea pentru o nouă viziune cu privire la acest tip de audit în spațiul Uniunii[4]. De altfel, la nivel

---

[1] Contact Committee of the Supreme Institutions of the European Union, *Audit Compendium. Cybersecurity in the EU and its Member States*, December 2020, pp. 9-12, AuditCommitehttps://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf, accesat în 12.02.2022.

[2] CGI, *Understanding Cybersecurity Standards*, April 2019, p. 11, https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf, accesat în 12.02.2022.

[3] P. Năstase (coordonator) ş.a., *Auditul şi controlul sistemelor informaționale*, Ed. Economică, Bucureşti, 2007, p. 55.

[4] Contact Committee of the Supreme Institutions of the European Union, *op. cit.*, p. 35.

global există preocupare sporită pentru *auditul intern şi extern de securitate cibernetică,* atât la nivelul instituțiilor private, cât şi la nivelul celor publice. Autoritățile publice cu atribuții în domeniul securității cibernetice au în vedere documentele ISACA potrivit cărora există trei linii de apărare a securității cibernetice: managementul organizației, managementul riscului şi auditul intern[5].

Dacă auditul intern urmăreşte cât de eficient este sistemul implementat, auditul extern verifică prin teste eficiența procedurilor de control încorporate în sistemul informatic, proceduri care trebuie să concretizeze exigențele standardelor specifice pentru a asigura folosirea eficientă a resurselor informaționale, securitatea cibernetică şi, nu în ultimul rând, atingerea obiectivelor entității auditate[6]. Având în vedere independența auditorului, el este cel care va stabili *in concreto* procedurile de control pe care le va aplica, folosindu-se în acest scop de cunoştințele, experiența, dar şi de intuiția sau, altfel spus, vocația sa profesională. Desigur, şi el trebuie să se raporteze de normele care reglementează auditul, inclusiv la *standardele privind auditul de securitate cibernetică*, iar în raportul de audit pe care-l întocmeşte la finalul misiunii de audit precizează la ce standarde s-a raportat. Standardele conferă *rigoare* misiunii de audit, fiind o premisă a abordării profesionale, responsabile a auditului, sporind încrederea în rezultatele acestuia.

Organizațiile cu activitate semnificativă în domeniul liniilor directoare în materie de audit al sistemelor informaționale sunt, în acest moment, următoarele:

- ISACA (Information Systems Audit and Control Association) prin Standardele COBIT
- IIA (Institute of Internal Auditors) prin Standardele IIA
- IFAC (International Federation of Accountants) prin Standardele ISA
- INTOSAI (International Organization of Supreme Audit Institutions) prin Standardele ISSAI

La standardele adoptate în cadrul acestor organizații se adaugă anumite standarde naționale care s-au impus în practica internațională, precum şi cele adoptate în cadrul unor grupuri de lucru[7].

În cele ce urmează vom trece în revistă principalele standarde privitoare la tehnologia informației, inclusiv cele privitoare la auditul sistemelor informaționale.

---

[5] ISACA, *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, 2017, p. 8, citat de Canadian Centre for Cybersecurity, *Cyber Security Audit Guide for the Government of Canada,* June 2020, p. 7, https://cyber.gc.ca/sites/default/files/2020-09/Cyber-Security-Audit-Guide_e.docx, accesat în 12.02.2022.

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

[7] Pentru detalii privind auditul sistemelor informatice/auditul cibernetic, a se vedea Curtea de Conturi a României, *Auditul sistemelor informatice. Manual,* Bucureşti, 2012, https://www.curteadeconturi.ro/uploads/25529564/77241a13/330b7f07/6c1123fc/16ba70a5/2eeb2cdf/0fbfb694/38bf227f/MANUAL_AUDIT_IT.pdf; Curtea de Conturi a României, *Ghidul de audit al sistemelor informatice*, Bucureşti, 2012, https://www.curteadeconturi.ro/uploads/ b3578fec/2e705397/8f5ff376/123728f6/08da8783/a7cf8c9a/974875d0/4f7867de/GHID_AUDIT_IT_CCR_24102012.pdf.

2. ISACA – Information Systems Audit and Control Association. Standardele COBIT

Information Systems Audit and Control Association – ISACA. Istoria ISACA începe în anul 1967 când un grup de specialişti în contabilitate şi audit, pornind de la problemele punctuale cu care se confruntau în activitatea lor curentă, au avut inițiativa constituirii unei organizații profesionale care să furnizeze informații şi îndrumări în domeniul auditului sistemelor informatice. Conceptul de audit al sistemelor de procesare automată a datelor (Electonic Data processing – EDP Audit) a fost lansat în 1968 de Institutul American al Contabililor Autorizați (American Institute of Certified Public Accountants – AICPA), moment urmat de constituirea Asociația Auditorilor EDP (EDP Auditors Association – EDPAA). Un rol important în dezvoltarea acestui tip de audit l-au avut marile firme de contabilitate, cunoscute ca The Big Eight[8], care au conştientizat impactul domeniului IT asupra activității lor. Acest grup-leader în materie de contabilitate şi audit a devenit astăzi The Big Four ca urmare a fuziunii ori dispariției de pe piață a unora dintre ele. The Big Four este format din companiile Deloitte, Ernst&Young, KPMG şi PwC şi acordă consultanță în contabilitate, finanțe, fiscalitate, asigurări, actuariat, management şi domeniul juridic, având un portofoliu important de clienți din toată lumea, atât din sectorul privat, cât şi din cel public.

În 1994 EDPAA devine Information Systems Audit and Control Association (Asociația pentru Auditul şi Controlul Sistemelor Informaționale), cunoscută sub acronimul *ISACA,* fiind cea mai cunoscută organizație profesională pe plan internațional în domeniul auditului de securitate cibernetică. ISACA este organizație neguvernamentală cu sediul la Schaumburg, Illinois, SUA, care reuneşte peste 165.000 de specialişti în domeniul auditului sistemelor informatice şi care activează în diferite domenii de activitate, în sectorul public şi privat, în peste 180 de state. Această diversitate le permite să facă schimb de puncte de vedere pe o varietate largă de subiecte profesionale[9], contribuind astfel la diseminarea bunelor practici în materie de audit IT. ISACA este prezentă şi în țara noastră prin filiala ISACA România[10].

Standardele COBIT. Arhitectura de auditare ISACA se constituie ca un ansamblu ierarhizat de elemente de ghidare care include următoarele niveluri şi componente: standarde, ghiduri de aplicare, proceduri şi resursele COBIT.

Standardele - definesc cerințele obligatorii pentru auditarea şi raportarea auditării sistemelor informatice. Potrivit Comitetului de Contact al Instituțiilor

[8] Grupul The Big Eight era format din Arthur Andersen, Arthur Young, Coopers & Lybrand, Deloitte Haskins and Sells, Ernst & Whinney, Peat Marwick Mitchell, Price Waterhouse şi Touche Ross.

[9] https://www.isaca.org/why-isaca/about-us, accesat în 14.02.2022.

[10] A se vedea activitatea ISACA România, www.isaca.ro.

Supreme de Audit din UE, Standardele COBIT elaborate de ISACA reprezintă un cadru de bune practici şi proceduri recunoscute pentru managementul IT, care ajută entitatea auditată să-şi îndeplinească obiectivele strategice prin utilizarea eficientă a resurselor şi minimizarea riscurilor IT. COBIT interconectează guvernanța întreprinderii şi guvernanța IT, această conexiune realizându-se prin legarea obiectivelor de business de cele de IT, definirea unor metrici şi modele pentru a măsura atingerea obiectivelor şi definirea responsabilităților managementului organizației şi managementului IT[11].

Ghidurile de aplicare - sunt ghiduri practice pentru aplicarea standardelor de auditare a sistemelor informatice.

Procedurile - cuprind exemple de proceduri pe care un auditor de sisteme informatice le-ar putea utiliza în cadrul unei misiuni de audit.

Resursele COBIT – sunt apreciate ca fiind *cele mai bune practici în materie* şi reprezintă un model general, detaliat, de controale şi tehnici de control, destinat unui mediu informatizat. Ele au un *rol diriguitor* în materie.

COBIT, acronim de la *Control Objectives for Information and related Technology*, prezintă activitățile de o manieră logică, uşor de gestionat. COBIT se concentrează în special pe controlul proceselor din cadrul organizației, oferind bune practici care vor ajuta la optimizarea investițiilor IT, funcționarea sistemului IT şi repere pentru corecția disfuncțiilor, slăbiciunilor sistemului. În acest context, COBIT constituie un instrument deosebit de util pentru auditori.

Cadrul de lucru COBIT a fost asimilat la nivel INTOSAI (Organizația Internațională a Instituțiilor Supreme de Audit) şi EUROSAI (Organizația Europeană a Instituțiilor Supreme de Audit) drept cadru de referință pentru auditurile desfăşurate de Instituțiile Supreme de Audit membre ale acestor organizații.

COBIT a fost aliniat şi armonizat cu următoarele standarde detaliate şi bune practici IT: COSO, ISO 27000, ITIL, Sarbanes-Oxley Act, BASEL II şi acționează ca un *integrator* al acestor standarde, sintetizând obiectivele principale sub un singur *cadru de referință general acceptat.*

Pentru a se ajunge la acest ansamblu[12], considerat de referință în materie, un prim demers a fost acela de a elabora un **Cod de etică profesională a auditorilor sistemelor informatice** care cuprinde un set de reguli de comportament ce ghidează conduita etică şi profesională a auditorilor certificați. Exercitarea acestei profesii supune următoarelor principii:

- implementarea standardelor şi procedurilor specifice de audit SI,
- seriozitate şi loialitate față de client,
- abținere de la activități ilegale,
- confidențialitatea informațiilor obținute în timpul misiunii de audit, cu excepția situației în care acestea sunt solicitate de autorități legale,

[11] Contact Committee of the Supreme Institutions of the European Union, *op. cit.*, p. 36.

[12] P. Năstase (coordonator) ş.a., *op. cit.*, pp. 17-21.

- independența auditorului ca premisă a corectitudinii şi lipsei de prejudecăți,
- profesionalism,
- informarea clientului cu privire la rezultatele auditului,
- susținerea informării asociaților/acționarilor/membrilor entității auditate pentru a creşte gradul de înțelegere a aspectelor referitoare la securitatea şi controlul sistemelor informatice, precum şi a încrederii în cadrul grupului.

După Codul de etică au fost elaborate **Standardele internaționale de audit al sistemelor informatice** care au permis uniformizarea internațională a practicilor de audit. Standardele oferă auditorului sistemelor informatice *un set de reguli şi principii* la care acesta se poate raporta în timpul misiunii de audit, pe de o parte, precum şi norme privitoare la obligația de a informa conducerea entității auditate şi alte persoane interesate despre desfăşurarea activităților şi practicile specifice acestui domeniu, pe de altă parte.

Pentru implementarea Standardelor au fost elaborate o serie de **Ghiduri metodologice** care oferă auditorului instrumente de aplicare a standardelor, proceduri de urmat în misiunile de audit.

Standardele internaționale de audit al sistemelor informatice privesc elementele specifice acestui tip de audit, elemente pe care le enumerăm în cele ce urmează.

Contractul de audit *(Audit Charter)* – misiunea de audit presupune încheierea prealabilă a contractului de audit, cunoscut şi sub denumirea de *scrisoare de angajament*. **Independența** *(Independence)* – este cheia de boltă a profesiei de auditor şi are două laturi: *independența profesională* prin care înțelegem independența față de unitatea auditată şi *independența organizațională* înțeleasă ca independență față de aria auditată.

Etica şi standardele profesionale *(Professional Ethics and Standards)* care se referă la faptul că auditorul trebuie să respecte *Codul etic elaborat de ISACA* şi *Standardele de audit* în vigoare la data efectuării misiunii de audit.

Competența profesională *(Professional Competence)* – auditorul trebuie să fie competent din punct de vedere profesional pentru a efectua misiunea de audit, să aibă aptitudinea şi cunoştințele necesare pentru aceasta; totodată, având în vedere că domeniul este caracterizat printr-o dinamică accentuată, auditorul trebuie să-şi mențină competența prin *educație şi formare continuă*, urmând cursuri de pregătire, participând la conferințe, workshop-uri, etc.

Planificarea *(Planning)* – auditorul trebuie să-şi planifice misiunea de audit în funcție de obiectivele acesteia, cu respectarea standardelor de audit şi a legislației în vigoare. Auditorul trebuie să stabilească o *strategie de audit bazată pe riscuri*, precum şi un *plan de audit* care să stabilească obiectivele auditului, întinderea misiunii de audit, durata acesteia, precum şi resursele necesare.

Evaluarea riscului în planificarea auditului *(Use of Risk Assesment in Audit Planning)* – planificarea misiunii de audit se face ținând cont riscurile sistemului auditat, dar şi de riscurile care planează asupra misiunii de audit.

Pragul de semnificație în audit *(Audit Materiality)* – există o relație invers proporțională între pragul de semnificație[13] şi riscul de audit, cu cât pragul de semnificație este mai scăzut riscul este mai mare şi invers.

Performanța activității de audit *(Performance of Audit Work)* – presupune:

- *supervizare* – şeful misiunii de audit va supraveghea echipa sa de specialişti pentru atingerea obiectivelor, respectarea standardelor şi legislației

- *documentare* – auditorul descrie în foile de lucru activitatea desfăşurată şi probele obținute

- *probele de audit* – tehnicile şi procedurile utilizate de auditor trebuie să conducă la obținerea de probe suficiente, relevante şi de încredere pentru atingerea obiectivelor auditului; *concluziile* se vor baza pe analiza şi interpretarea acestor probe.

Raportarea *(Reporting)* – la finalul misiunii, auditorul va întocmi *Raportul de audit* în care menționează, printre altele, entitatea auditată, destinatarii raportului şi eventualele restricții de circulație a acestuia, concluziile şi recomandările pentru remedierea deficiențelor constatate. Raportul se semnează de auditor şi trebuie realizat în termenul stabilit prin contractul de audit sau scrisoarea de angajament. Raportul cuprinde opinia auditorului cu privire la obiectivele misiunii de audit.

Urmărirea recomandărilor din Raportul de audit *(Follow up Activities)* – presupune revenirea auditorului la entitatea auditată pentru a evalua măsurile luate de conducere pentru punerea în practică a recomandărilor.

Frauda şi eroarea *(Irregularities and Illegal Acts) – pentru a reduce riscul de audit la un nivel acceptabil*, auditorul trebuie să evalueze riscul apariției unor fraude sau erori. Auditorul trebuie să fie rezervat, să manifeste o atitudine de scepticism pe durata misiunii sale, ținând cont de posibilitatea existenței unor acte ilegale.

Guvernanța IT *(IT Governance)* – presupune următoarele aspecte:

- evaluarea de către auditor a sistemului IT al entității auditate şi dacă acesta susține obiectivele şi strategia entității,

- evaluarea eficienței utilizării resursele sistemului informațional al entității şi performanța managementului IT,

- analiza managementului riscurilor asociate sistemelor IT.

Utilizarea informațiilor obținute de la alți experți *(Using the Work of Other Experts)* – pentru obținerea probelor de audit auditorul trebuie să folosească dacă este cazul experiența şi competența altor experți, precum consultant managerial, expert IT, expert fiscal, expert contabil, etc., să-i consulte, să le ceară părerea, dar

[13] Din considerente de timp şi de cost, auditorul nu examinează toate informațiile la care are acces pentru a-şi culege probele de audit, ci foloseşte tehnica eşantionării. El acceptă încă de la început că va lucra cu o anumită marjă de eroare şi trebuie să stabilească care este mărimea erorii pe care o va accepta. Dimensiunea marjei de eroare determină pragul de semnificație definit ca limita de la care auditorul va trebui să detecteze eventualele anomalii semnificative, mărimea şi natura acestora. A evalua ce este semnificativ, esențial este o problemă de judecată profesională, iar alegerea pragului de semnificație în cadrul unei misiuni de audit de securitate cibernetică nu este un demers facil.

opiniile acestora vor fi evaluate ținând cont de pregătirea şi experiența lor profesională, precum şi de independența lor.

Probele de audit *(Audit Evidence)* – auditorul trebuie să obțină probe suficiente pentru fundamentarea concluziilor din raportul de audit.

3. IIA – Institute of Internal Auditors/Standardele IIA

Institute of Internal Auditors – IIA. Fondată în anul 1941, The IIA este o organizație neguvernamentală, o asociație profesională cu sediul în Lake Mary, Florida, SUA, având un număr de peste 200.000 de membri şi reprezentanțe în mai mult de 170 de țări. Este o autoritate recunoscută ca important formator, leader în certificare, instruire, cercetare ştiințifică şi ghidare tehnologică pentru profesia de auditor pe plan mondial. În domeniul auditului IT, IIA promovează cunoştințe specializate şi suport modern, în concordanță cu tendințele şi evoluțiile pe plan mondial, contribuind la accelerarea extinderii şi adaptării misiunilor de audit la cerințele impuse de existența unui mediu de audit informatizat pe scară largă[14].

Standardele IIA. IIA furnizează standarde, dar şi numeroase resurse suplimentare pentru a sprijini activitatea de audit: ghiduri de implementare a celor mai bune practici, studii de caz şi alte instrumente integrate în cadrul de lucru IPPF (*International Professional Practices Framework*).

În domeniul auditului IT, liniile directoare de audit *GTAG (Global Technology Audit Guidelines)* abordează probleme legate de managementul tehnologiei informației, controlul şi securitatea informației. Seria GTAG constituie o resursă pentru auditori, tratează riscurile asociate diferitelor tehnologii şi recomandă practicile pentru reducerea impactului acestora.

Liniile directoare sunt structurate pe următoarele categorii de probleme:
GTAG PG-15: Securitatea informației
GTAG PG-14: Auditul aplicațiilor dezvoltate de utilizatori
GTAG PG-13: Prevenirea şi detectarea fraudei într-un mediu informatizat
GTAG PG-12: Auditul proiectelor IT
GTAG PG-11: Elaborarea Planului de Audit IT
GTAG PG-10: Managementul continuității
PG GTAG-9: Managementul identității şi al accesului
PG GTAG-8: Auditarea controalelor de aplicație
PG GTAG-7: Externalizarea tehnologiei informației
PG GTAG-6: Managementul şi auditul vulnerabilităților IT
GTAG PG-5: Managementul şi auditul riscurilor privind confidențialitatea
GTAG-4: Managementul auditului IT

[14] Pentru detalii privind activitatea organizației, a se vedea https://www.theiia.org/.

PG GTAG-3: Audit continuu: Implicații pentru asigurare, monitorizare şi evaluare a riscurilor

PG GTAG-2: Controale privind managementul schimbării

PG GTAG-1: Controale IT

4. IFAC - International Federation of Accountants/Standardele ISA

International Federation of Accountants – IFAC. Este o organizație neguvernamentală care fost constituită în anul 1977 la München, Germania, având 63 de membri fondatori din 51 de state, cu scopul de a consolida profesia la nivel global prin: dezvoltarea de standarde internaționale în activitatea de audit şi asigurare, contabilitate în sectorul public, etică şi educație pentru profesia de contabil; colaborare şi cooperare între membrii săi; colaborare şi cooperare cu alte organizații internaționale; reprezentarea intereselor profesiei contabile pe plan internațional. Astăzi organizația are 180 de membri din 135 de state, reunind peste 3 milioane de specialişti în contabilitate şi audit[15].

La prima reuniune a organizației din 1977, a fost adoptat un program de acțiune în 12 puncte pentru primii 5 ani de activitate, care însă sunt valabile şi astăzi, după cum urmează[16]:

1. elaborarea de linii directoare pentru activitatea de audit,
2. elaborarea de principii care să se regăsească în Codurile etice ale membrilor IFAC, perfecționarea şi dezvoltarea acestora,
3. dezvoltarea de programe pentru educația şi formarea profesională a contabililor,
4. colectarea, analiza, cercetarea şi diseminarea informațiilor privind managementul practicilor în contabilitatea publică,
5. evaluarea, dezvoltarea şi raportarea privind managementul financiar, alte tehnici şi proceduri de management,
6. efectuarea de studii privind evaluarea şi răspunderea contabililor,
7. promovarea unor relații mai strânse cu utilizatorii situațiilor financiare, dar şi cu instituții din educație şi formare profesională, sindicate, asociații de comerț, industrie, guverne,
8. menținerea bunelor relații cu organizațiile regionale şi explorarea posibilităților de a constitui alte organizații regionale, asistență pentru constituirea şi dezvoltarea acestora,
9. dialog permanent între membrii IFAC şi alte organizații interesate,

[15] Din România sunt membre IFAC: Camera Auditorilor Financiari din România şi Corpul Experților Contabili şi Contabililor Autorizați din România.

[16] https://www.ifac.org/who-we-are/our-purpose, accesat în 14.02.2022.

10. schimb de informații tehnice, materiale educaționale şi publicații profesionale,

11. organizarea periodică a unui Congres internațional,

12. extinderea IFAC.

Standardele ISA. În cadrul IFAC au fost constituite grupuri de lucru pentru elaborarea unor standarde internaționale, după cum urmează:

- IAASB – International Auditing and Assurance Standards Board
- IAESB – International Accounting Education Standards Board
- IESBA – International Ethics Standards Board for Accountants
- IPSASB – International Public Sector Accounting Standards Board

IAASB (Consiliul pentru Standarde Internaționale de Audit şi Asigurare) a adoptat Standardele Internaționale de Audit – ISA care au abordat probleme specifice celor două domenii de activitate. În ceea ce priveşte domeniul auditului, au fost adoptate standarde precum:

ISA 300 – Planificarea auditului

ISA 315 – Cunoaşterea entității şi mediului său şi evaluarea riscurilor de deturnare semnificativă

ISA 400 – Evaluarea riscurilor şi controlul intern

ISA 402 – Considerente de audit referitoare la entitățile care apelează la firme de servicii

5. INTOSAI - International Organization of Supreme Audit Institutions/Standardele ISSAI

International Organization of Supreme Audit Institutions – INTOSAI. Organizația Internațională a Instituțiilor Supreme de Audit sau INTOSAI este o organizație nonguvernamentală profesională, independentă, autonomă, nonpolitică cu activitate permanentă, a cărei constituire a fost hotărâtă în anul 1953, la Congresul instituțiilor supreme de audit, de la Havana, Cuba, congres la care au fost reprezentate 34 de state şi organizații.

Organizația reuneşte instituțiile supreme de audit ale statelor şi organizațiilor internaționale şi are ca scop[17]:

- sprijinirea dezvoltării instituțiilor supreme de audit, cooperarea şi creşterea continuă a performanței şi credibilității acestor instituții,
- creşterea transparenței privind fondurile publice,
- promovarea schimbului de idei, cunoştințe şi experiență,
- stabilirea standardelor de audit pentru sectorul public,

[17] https://www.intosai.org/about-us/overview, accesat în 14.02.2022.

- promovarea bunei guvernări la nivel național, creşterea eficienței şi eficacității constituirii, repartizării şi utilizării fondurilor publice şi punerea acestora în slujba cetățenilor,
- combaterea corupției,
- reprezentarea instituțiilor supreme de audit pe plan internațional.

În România, instituția supremă de audit public este Curtea de Conturi a României, membră INTOSAI. În cadrul ei funcționează şi Autoritatea de Audit care verifică modul de utilizare a fondurilor europene alocate României. Instituții similare există în toate statele membre ale Uniunii Europene, dar şi în state terțe, nemembre UE. La nivelul UE îşi desfăşoară activitatea Curtea de Conturi a UE care auditează constituirea, repartizarea şi utilizarea fondurilor Uniunii, instituție care este membră cu drepturi depline a INTOSAI.

INTOSAI are sediul la Viena, Austria, şi are 196 de membri cu drepturi depline, 5 membri asociați şi 2 membri afiliați. Organizația acordă statutul de membru afiliat organizațiilor regionale care reunesc instituții supreme de audit, înființate în scopul promovării cooperării profesionale şi tehnice a membrilor la nivel regional. EUROSAI, a cărei membră este şi Curtea de Conturi a României, este membru afiliat al INTOSAI alături de alte 6 organizații regionale: AFROSAI, ARABOSAI, ASOSAI, CAROSAI, OLACEFS şi PASAI.

Standardele ISSAI. Standardele internaționale adoptate în cadrul INTOSAI – Standardele ISSAI (International Standards of Supreme Audit Institutions**)** – creează premisele pentru buna funcționare şi conduita profesională a Instituțiilor Supreme de Audit, formulând şi principiile fundamentale *în domeniul auditului entităților publice.* Aceste standarde îşi propun să asigure: calitate, credibilitate, transparență, responsabilitate şi limbaj comun în materie de audit public. Alături de standardele ISSAI, liniile directoare INTOSAI (*INTOSAI GOV*) oferă asistență autorităților publice cu privire la administrarea corectă a fondurilor publice[18].

6. COSO – Comittee of Sponsoring Organizations/Standardele COSO

Comittee of Sponsoring Organizations – COSO. Organizația a fost constituită în anul 1985 pentru a susține financiar Comisia Națională pentru Raportare Frauduloasă (Național Commission on Fraudulent Financial Reporting), comisie care avea ca scop identificarea cauzelor raportării financiare frauduloase şi furnizarea de recomandări instituțiilor din sectorul public, instituțiilor de învățământ, autorităților de reglementare din domeniu. Comisia, instituție de drept privat, a fost susținută financiar de cinci asociații profesionale americane: AAA (American Accounting Association), AICPA (American Institute of Certified Public

[18] https://www.intosai.org/focus-areas/audit-standards, accesat în 14.02.2022.

Accountants), FEI (Financial Executives International), IIA (Institute of Internal Auditors) şi IMA (National Association of Accountants).

Activitatea COSO vizează susținerea membrilor în efortul de creştere a performanței prin creşterea eficienței controlului intern, managementul riscurilor, guvernanță şi descurajarea fraudei, acordând atenție activității de control în mediile digitalizate, fiind recunoscută la nivel global ca autoritate în aceste domenii.

Standardele COSO. În ceea ce priveşte abordarea auditului bazată pe risc, un model general acceptat şi preferat pentru evaluarea controalelor interne este *Internal Control Integrated Framework,* elaborat de *Comittee of Sponsoring Organizations of the Treadway Commission (COSO)* în anul 1992. În anul 2004 acest model a fost perfecționat pentru a oferi un cadru de management al riscurilor acceptat pe scară largă, care include principii cheie, concepte, un limbaj comun privind riscurile şi ghiduri clare pentru implementare. Această direcție nouă, numită *Enterprise Risk Management Integrated Framework,* furnizează patru categorii de obiective organizaționale şi opt componente interrelaționate ale managementului eficace al riscului[19].

ISO – International Organization for Standardization/Standardele ISO

International Organization for Standardization – **ISO**. Organizația internațională pentru standardizare, cunoscută sub acronimul ISO, şi-a început activitatea în anul 1947, cu scopul de a elabora standarde de referință în diferite domenii de activitate şi de a le disemina la nivel internațional. Constituirea ei a fost hotărâtă în 1946, la Londra, cu prilejul Congresului internațional privind standardizarea, un an mai târziu începându-şi activitatea. Este o organizație neguvernamentală, independentă, care reuneşte 167 de organizații naționale cu preocupări în domeniul standardizării, având sediul la Geneva, Elveția.

Standardele reprezintă ghiduri de bune practici pentru desfăşurarea diferitelor activități, iar diseminarea lor contribuie la abordarea unitară la nivel global a problematicii specifice acestora. Standardele sunt rodul cooperării, dar în acelaşi timp ele sunt baza, platforma comună care asigură premisele cooperării viitoare, un limbaj comun care asigură identificarea soluțiilor pentru rezolvarea problemelor cu care se confruntă specialiştii din diferite domenii. În cadrul ISO au fost adoptate standarde pentru cele mai variate domenii de activitate, de la mecanică şi electrotehnică, la energie nucleară şi tehnologia informației[20].

---

[19] Pentru detalii, a se vedea https://www.coso.org/Pages/guidance.aspx.

[20] Pentru detalii privind istoricul şi activitatea organizației, a se vedea ISO, *Friendship among equals. Recollections from ISO s first fifty years*, Geneva, 1997, https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf.

În domeniul IT, în cadrul ISO a fost adoptat pachetul ISO 27000/Securitatea informației[21] care cuprinde:

ISO 27000 Securitatea informației

ISO/CEI 27001 Information Security Management System (ISMS), înlocuieşte BS7799-2

ISO/CEI 27002 Cod de bune practici în ISMS. Nou număr pentru ISO 17799

ISO/CEI 27003 Ghid de implementare a ISMS.

ISO/CEI 27004 Ghid pentru gestionarea, măsurarea şi metrica securității informației.

ISO/CEI 27005 Ghid pentru managementul riscului în securitatea informației.

Standardele ISO sunt adoptate, traduse şi difuzate în România de ASRO - Asociația de Standardizare din România care participă prin specialiştii săi în cadrul comitetelor tehnice internaționale ale ISO. ASRO este o asociație, persoană juridică română de drept privat, de interes public, fără scop lucrativ, neguvernamentală şi apolitică care funcționează în baza prevederilor Legii nr. 163/2015 privind standardizarea națională şi Ordonanței Guvernului nr. 26/2000 cu privire la asociații şi fundații. ASRO este platforma națională pentru adoptarea şi distribuirea standardelor internaționale şi europene la nivel național, precum şi a informațiilor despre standarde în toate domeniile de activitate[22]. Organizația este membru cu drepturi depline a ISO din anul 1950 şi a Comitetului European de Standardizare din anul 2006.

7. Standarde naționale de referință în auditul sistemelor informatice. SUA/Standardele Sarbanes-Oxley (SOX)

Ca reacție la eşecul unor misiuni de audit, reglementarea profesiei de auditor s-a bucurat de o atenție deosebită în SUA. Scandalul ENRON a antrenat adoptarea de către Congresul american a *U.S. Sarbanes-Oxley (SOX) Act (2002)*. Elementele principale de noutate aduse de această lege sunt:

- independența auditorilor financiari,
- responsabilitatea managementului şi a controlului intern pentru acuratețea, documentarea şi întocmirea rapoartelor financiare,
- răspunderea penală a acestora în cazul încălcării obligațiilor prevăzute de lege,
- constituirea unei autorități care să supravegheze activitatea de audit public, să adopte standarde de audit, să vegheze la respectarea independenței auditorilor şi asigurarea calității rapoartelor de audit,

[21] Pentru detalii, a se vedea https://www.27000.org/.

[22] La nivel european activitatea de standardizare este reglementată de Regulamentul 1025_2012.

- implementarea unor proceduri de validare şi de evaluare a controalelor, inclusiv în ceea ce priveşte controalele IT; sistemul informatic trebuie să susțină procesul de raportare în conformitate cu SOX.

Seria de **Linii directoare GAIT** descrie relațiile dintre riscurile afacerii, controalele cheie asociate proceselor afacerii, controalele automate şi controalele cheie din cadrul controalelor generale IT. Este *o abordare bazată pe risc* pentru auditarea controalelor generale IT ca parte a sistemului de audit intern al entității, destinată identificării deficiențelor, în conformitate cu Secțiunea 404 din Sarbanes-Oxley Act (SOX).

Această lege a fost criticată pentru costurile pe care le induce, dar potrivit altor opinii aceste costuri sunt contrabalansate de avantajele pe care le procură corectitudinea situațiilor financiare[23].

Concluzii

În cadrul unor organizații internaționale, au fost adoptate standarde pentru diferite domenii de activitate, printre care şi cele privind tehnologia informației, inclusiv standarde privind auditul securității sistemelor informaționale. În acest articol am prezentat organizațiile internaționale cu activitate relevantă în domeniul standardizării în domeniul IT şi al auditului de securitate cibernetică. Alături de standardele adoptate în cadrul acestor organizații, există şi alte standarde adoptate de alte organizații ori grupuri de lucru.

Un rol important îl are educația despre standardizare, astfel încât profesioniştii din diferite domenii să includă în activitatea lor standardele ca o premisă a performanței activității desfăşurate. Educația pentru standardizare este în atenția UE, în cadrul ei fiind elaborate: Politica Comitetului European de Standardizare în domeniul educației pentru standardizare, Masterplanul Educație despre standardizare şi Planul de implementare a Masterplanului Educație despre standardizare[24]. Deşi s-ar părea că standardele interesează doar inginerii, proiectanții sau specialiştii IT, cunoştințe despre standarde ar trebui să aibă specialiştii din toate domeniile reglementate de standarde, dar şi cei care activează în domenii conexe, inclusiv juriştii, pentru că abordarea realităților lumii contemporane nu mai poate fi una de nişă, ci presupune o viziune holistică, interdisciplinară, cu atât mai mult cu cât vorbim despre *cybersecurity* şi *cybercrime*.

---

[23] Legal Information Institute, *Sarbanes-Oxley Act*, https://www.law.cornell.edu/wex/sarbanes-oxley_act, accesat în 14.02.2022.

[24] Pentru detalii, a se vedea https://www.cencenelec.eu/.

Bibliografie

1. Canadian Centre for Cybersecurity, *Cyber Security Audit Guide for the Government of Canada,* June 2020, p.7, https://cyber.gc.ca/sites/default/files/2020-09/Cyber-Security-Audit-Guide_e.docx

2. CGI, *Understanding Cybersecurity Standards*, April 2019, https://www.cgi.com/sites/default/files/2019-08/cgi-understanding-cybersecurity-standards-white-paper.pdf

3. Contact Committee of the Supreme Institutions of the European Union, *Audit Compendium. Cybersecurity in the EU and its Member States*, December 2020, AuditCommitehttps://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EN.pdf

4. Curtea de Conturi a României, *Auditul sistemelor informatice. Manual,* Bucureşti, 2012, https://www.curteadeconturi.ro/uploads/25529564/77241a13/330b7f07/6c1123fc/16ba70a5/2eeb2cdf/0fbfb694/38bf227f/MANUAL_AUDIT_IT.pdf

5. Curtea de Conturi a României, *Ghidul de audit al sistemelor informatice*, Bucureşti, 2012, https://www.curteadeconturi.ro/uploads/b3578fec/2e705397/8f5ff376/123728f6/08da8783/a7cf8c9a/974875d0/4f7867de/GHID_AUDIT_IT_CCR_24102012.pdf

6. ISO, *Friendship among equals. Recollections from ISO s first fifty years*, Geneva, 1997, https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf

7. Legal Information Institute, *Sarbanes-Oxley Act*, https://www.law.cornell.edu/wex/sarbanes-oxley_act

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

9. https://www.isaca.org/why-isaca/about-us

10. www.isaca.ro

11. https://www.theiia.org/

12. https://www.ifac.org/who-we-are/our-purpose

13. https://www.intosai.org/about-us/overview

14. https://www.intosai.org/focus-areas/audit-standards

15. https://www.coso.org/Pages/guidance.aspx

16. https://www.iso.org/standards.html

17. https://www.27000.org/

18. https://www.cencenelec.eu/