

## STANDARDUL INTERNAȚIONAL DE AUDIT 401

### AUDITUL ÎNTR-UN MEDIU CU SISTEME INFORMATIZATE

#### CUPRINS

Introducere.....	1-3
Aptitudini și competență.....	4
Planificare.....	5-7
Evaluarea riscului.....	8-10
Proceduri de audit.....	11-12

Standardele Internaționale de Audit (ISA) sunt utilizate în auditarea situațiilor financiare. ISA se utilizează, de asemenea, adaptate conform necesităților, la auditarea altor informații și servicii conexe.

ISA conține principiile de bază și procedurile esențiale (identificate după fontul literei cu care sunt tipărite, și anume, caractere aldine), precum și recomandările aferente, sub forma materialelor explicative și a altor materiale. Principiile de bază și procedurile esențiale trebuie să fie interpretate în contextul materialelor explicative, și al altor materiale care oferă îndrumări privind modul de aplicare.

Pentru înțelegerea și aplicarea principiilor de bază și a procedurilor esențiale, precum și a recomandărilor aferente trebuie să se ia în considerare întregul text al ISA, incluzându-se și materialele explicative și celelalte materiale conținute în ISA, și nu doar textul tipărit cu caracter aldine.

În situații excepționale, un auditor financiar poate considera necesară abaterea de la ISA, cu scopul de a realiza mai eficient obiectivul unui audit financiar. Când apar astfel de situații, auditorul financiar trebuie să fie pregătit să justifice această abatere.

ISA trebuie să se aplice doar aspectelor semnificative.

Perspectiva Sectorului Public (PSP) emisă de Comitetul pentru Sectorul Public al Federației Internaționale a Contabililor este stabilită la sfârșitul fiecărui ISA. Când nu este adăugată nici o PSP, ISA se aplică sectorului public sub toate aspectele semnificative.

## Introducere

1. Scopul acestui Standard Internațional de Audit (ISA) este să stabilească reguli și să ofere recomandări pentru procedurile ce trebuie urmate atunci când este efectuat un audit într-un mediu cu sisteme informatizate (CIS<sup>1</sup>). Pentru scopurile ISA, un mediu CIS există atunci când un calculator de orice tip sau mărime este implicat în prelucrarea de către entitate a informațiilor financiare cu semnificație pentru audit, indiferent dacă acel calculator este operat de entitate sau de o terță parte.
2. **Auditorul trebuie să ia în considerare modul în care un mediu CIS afectează auditul.**
3. Obiectivul general și sfera unui angajament de audit nu se modifică într-un mediu CIS. Cu toate acestea, utilizarea unui calculator modifică modul de procesare, stocare și comunicare al informațiilor financiare și poate afecta sistemul contabil și pe cel de control intern utilizate de entitate. În consecință, un mediu CIS poate afecta:
  - Procedurile utilizate de auditor pentru a obține o înțelegere suficientă a sistemelor de contabilitate și control intern.
  - Considerentele cu privire la riscul inerent și riscul de control prin care auditorul obține evaluarea riscului.
  - Proiectarea și desfășurarea de către auditor a testelor controalelor și a procedurilor de fond adecvate îndeplinirii obiectivului auditului.

## Aptitudini și competență

4. **Auditorul trebuie să aibă cunoștințe suficiente despre CIS pentru a planifica, a conduce, a supraveghea și a revizui activitatea desfășurată. Auditorul trebuie să ia în considerație dacă într-un audit sunt necesare aptitudini CIS specializate.** Acestea ar putea fi necesare pentru:
  - Înțelegerea suficientă a sistemelor contabil și de control intern afectate de mediul CIS.
  - Determinarea efectului mediului CIS în evaluarea riscului general și a riscului în stabilirea nivelului soldului contului și a clasei tranzacțiilor.
  - Planificarea și efectuarea testelor adecvate ale controalelor, precum și a procedurilor de fond.

Dacă sunt necesare aptitudini specializate, auditorul trebuie să consulte un profesionist care posedă astfel de aptitudini și care poate face parte fie din personalul auditorului, fie din afara acestuia. **Dacă este planificată utilizarea unui astfel de profesionist, auditorul trebuie să obțină suficiente probe de audit adecvate, evidențiind faptul că o astfel de activitate corespunde scopurilor auditului, în concordanță cu ISA 620, “Utilizarea serviciilor unui expert”.**

---

<sup>1</sup> Acest termen este utilizat pe parcursul prezentului ISA, în loc de procesarea electronică a datelor (EDP) utilizat în ISA anterior “Activități de audit într-un mediu EDP”. Declarația relevantă privind practica internațională de audit, revizuită și emisă ulterior acestui ISA folosește termenul „medii de tehnologie a informației (IT)”.

### Planificare

5. **În concordanță cu ISA 400 “Evaluarea riscurilor și controlul intern”, auditorul trebuie să obțină o înțelegere suficientă a sistemului contabil și a sistemului de control intern pentru a planifica auditul și pentru a dezvolta o abordare eficientă a acestuia.**
6. **În planificarea părților din audit ce pot fi afectate de mediul CIS al clientului, auditorul trebuie să înțeleagă semnificația și complexitatea activităților CIS, precum și disponibilitatea datelor ce se utilizează în audit.** Această înțelegere include aspecte, cum ar fi:
  - Importanța și complexitatea procesării computerizate în fiecare aplicație contabilă semnificativă. Importanța se referă la pragul de semnificație al aserțiunilor din situațiile financiare afectate de procesarea computerizată. O aplicație poate fi considerată complexă atunci când, de exemplu:
    - Volumul tranzacțiilor este de așa natură încât utilizatorii găsesc că este dificil să identifice și să corecteze erorile în timpul procesării.
    - Computerul generează automat, direct către o altă aplicație, tranzacții sau intrări semnificative.
    - Computerul execută calcule complicate ale informațiilor financiare și/sau generează automat tranzacții sau intrări semnificative care nu pot fi (sau nu sunt) validate în mod independent.
    - Tranzacțiile sunt schimbate electronic cu alte organizații (ca în sistemele de transferuri electronice de date EDI) fără o revizuire manuală a proprietăților și rezonabilității.
  - Structura organizațională a activităților CIS ale clientului și măsura concentrării sau repartizării procesului computerizat în cadrul întregii entități, în mod special în cazul în care acestea pot afecta separarea sarcinilor.
  - Disponibilitatea datelor. Documentele primare, anumite fișiere și alte informații importante ce pot fi cerute de către auditor pot exista doar pentru o scurtă perioadă de timp sau doar într-o formă electronică. Mediul CIS al clientului poate genera o raportare internă ce poate fi utilă în efectuarea testelor de fond (în particular a procedurilor analitice). Potențialul pentru utilizarea tehnicilor de audit asistate de calculator poate permite creșterea eficienței performanței procedurilor de audit sau poate permite auditorului să aplice în mod economic anumite proceduri unei întregi clase de conturi și tranzacții.
7. **Când mediul CIS este semnificativ, auditorul trebuie să obțină, de asemenea, o înțelegere a mediului CIS și dacă acesta poate influența evaluarea riscurilor inerent și de control.** Natura riscurilor și caracteristicile controlului intern în mediile CIS includ următoarele:
  - Lipsa dovezilor tranzacției. Unele CIS-uri sunt proiectate astfel încât o dovadă completă utilă scopurilor auditului în ceea ce privește tranzacția ar putea exista doar pentru o scurtă perioadă de timp sau doar într-o formă electronică. Acolo unde un sistem complex de aplicații execută un număr mare de pași de procesare, acesta nu poate constitui o dovadă completă. În consecință, erorile cuprinse în programul logic al unei aplicații pot fi dificil

de detectat în timp util prin proceduri manuale (proceduri efectuate de utilizator).

- Procesarea uniformă a tranzacțiilor. Procesarea computerizată prelucrează în mod uniform tranzacțiile similare ce au aceleași instrucțiuni de procesare. Astfel, erorile de redactare asociate în mod obișnuit procesării manuale sunt aproape eliminate. Dimpotrivă, erorile de programare (sau alte erori sistematice în hardware sau software) vor avea ca rezultat, în mod normal, prelucrarea incorectă a tuturor tranzacțiilor.
- Lipsa separării funcțiilor. Unele proceduri de control care, în mod normal, sunt executate în sistem manual de indivizi separați pot fi concentrate în CIS. În acest fel, un individ care are acces la programe, proceduri sau date computerizate se poate găsi în situația de a executa funcții incompatibile.
- Potențialul de apariție a erorilor și neregularităților. Potențialul apariției erorilor umane în dezvoltarea, menținerea și executarea CIS poate fi mai mare decât în sistemul manual, parțial datorită nivelului de detaliu, inerent în aceste activități. De asemenea, potențialul indivizilor de a câștiga accesul neautorizat la date sau de a altera datele fără o dovadă vizibilă poate fi mai mare în CIS decât în sistemele manuale.
- În plus, diminuarea implicării umane în manevrarea tranzacțiilor procesate în CIS poate reduce potențialul neobservării erorilor și neregularităților. Erorile sau neregularitățile ce apar în timpul proiectării sau modificării programelor de aplicație, sau a sistemelor software pot rămâne nedetectate pentru o lungă perioadă de timp.
- Inițierea sau executarea tranzacțiilor. CIS poate include capacitatea de a iniția sau cauza execuția anumitor tipuri de tranzacții, în mod automat. Autorizarea acestor tranzacții sau proceduri poate să nu fie documentată în același mod cu acelea dintr-un sistem manual, iar autorizarea de către management a acestor tranzacții poate fi implicită prin modul în care a fost proiectat CIS-ul și pentru modificările ulterioare ale acestuia.
- Dependența de alte controale prin procesări computerizate. Procesarea computerizată poate produce rapoarte și alte elemente care sunt utilizate în efectuarea procedurilor manuale de control. Eficacitatea acestor proceduri manuale de control poate fi dependentă de eficiența controalelor asupra exhaustivității și exactității procesării computerizate. În schimb, eficacitatea și operarea consecventă a controalelor asupra procesării tranzacțiilor în aplicațiile computerizate depind, adesea, de eficiența controalelor CIS generale.
- Potențial de supraveghere sporită realizată de conducere. CIS poate oferi conducerii o varietate de instrumente analitice care pot fi folosite pentru a revizui și supraveghea operațiunile entității. Disponibilitatea acestor controale suplimentare, dacă este nevoie, poate ajuta la sporirea întregii structuri de control intern.
- Potențial de utilizare a tehnicilor de audit asistate de calculator. Procesarea și analizarea unei cantități mari de date, utilizând calculatoarele, poate oferi auditorului oportunități de aplicare a tehnicilor și instrumentelor generale de audit asistate de calculator sau specializate în executarea testelor de audit.

Atât riscul, cât și controalele introduse ca rezultat al acestor caracteristici ale CIS au un impact potențial în evaluarea de către auditor a riscului și a naturii, duratei și întinderii procedurilor de audit.

#### Evaluarea riscurilor

8. **În concordanță cu ISA 400 “Evaluarea riscurilor și controlul intern”, auditorul trebuie să facă o evaluare a riscului inerent și a riscului de control pentru aserțiunile semnificative din situațiile financiare.**
9. Riscul inerent și riscul de control într-un mediu CIS pot avea atât un efect cuprinzător, cât și un efect specific asupra conturilor în ceea ce privește probabilitatea de apariție a unor denaturări semnificative, după cum urmează:
  - Riscurile pot rezulta din deficiențe ale activităților generale din CIS, cum ar fi dezvoltarea și întreținerea programelor, suportul sistemelor software, operații, securitatea fizică a CIS și controlul asupra accesului la programe utilitare speciale. Aceste deficiențe tind să aibă un impact universal asupra tuturor sistemelor de aplicații care sunt procesate computerizat.
  - Riscurile pot crește potențialul de apariție a erorilor și activităților frauduloase în aplicațiile specifice, în bazele de date specifice sau în fișierele master, sau în activitățile specifice de procesare. De exemplu, erorile sunt comune în sistemele ce efectuează operații logice sau calcule complexe, sau sisteme care trebuie să facă față multor condiții diferite ce sunt considerate excepții. Sistemele ce controlează sumele plătite în numerar sau alte active lichide sunt susceptibile acțiunilor frauduloase efectuate de utilizatori, sau de personalul CIS.
10. Pe măsură ce apar noi tehnologii CIS, acestea sunt frecvent utilizate de clienți pentru a construi sisteme computerizate complexe care pot include legături de la cele mai mici la cele mai importante, baze de date distribuite, procesare finală la utilizator, sisteme de conducere a afacerii care furnizează informații direct în sistemele contabile. Astfel de sisteme sporesc complexitatea generală a CIS, precum și complexitatea aplicațiilor specifice ce sunt afectate de aceste sisteme. Ca rezultat, sistemele pot spori riscul și solicită atenție suplimentară.

#### Proceduri de audit

11. **În conformitate cu ISA 400 “Evaluarea riscurilor și controlul intern”, auditorul trebuie să ia în considerare mediul CIS în proiectarea procedurilor de audit pentru a reduce riscul de audit la un nivel acceptabil de scăzut.**
12. Obiectivele specifice ale auditorului nu se modifică dacă datele contabile sunt procesate manual sau cu ajutorul computerului. Cu toate acestea, metodele de aplicare a procedurilor de audit pentru colectarea probelor pot fi influențate de metodele de procesare computerizată. Auditorul poate utiliza fie procedurile manuale de audit, tehnici de audit asistate de calculator, fie o combinație între cele două pentru a obține suficiente probe. Oricum, în unele sisteme de contabilitate, care folosesc un computer pentru procesarea aplicațiilor semnificative, poate fi dificil sau imposibil ca auditorul să obțină anumite date pentru inspecție, investigație, sau confirmare fără asistență computerizată.

AUDIT