

AUDITUL SISTEMELOR INFORMATICE

Ec. Ioana Florentina CHIȘ, Lector univ. dr. Liliana Simona Todor¹

Abstract

The on - site intervention stage has resulted in field testing of all the auditor's actions, based on the „ On- site intervention done based on a fixed schedule”, using various sampling techniques, check lists, tests, interviews and relation notes, items that have constituted audit samples and are the base of the FIAP and FCRI documentations, and which will be part of the auditory's report on the „Organization and functioning of the It departments in the S.N.L.O sub-units”.

Cuvinte cheie: misiune de audit intern, FIAP, FCRI, subunități S.N.L.O.

INTRODUCERE

Având o importanță majoră în cadrul oricărei organizații, auditul intern este activitatea independentă și obiectivă care dă entității o asigurare în ceea ce privește gradul de control asupra operațiunilor, o îndruma pentru a-i îmbunătăți operațiunile, și contribuie la adaugarea unui plus de valoare.

Astfel, pentru a ajuta organizația să își atingă obiectivele, auditul intern evaluând procesele ce au loc la nivelul departamentului IT, printr-o abordare sistematică și metodică, oferă ulterior propuneri pentru a-i consolida eficacitatea.

Auditorii interni au cunostinte legate de principalele riscuri și controale IT și de tehnicile de audit disponibile pentru a-și exercita activitatea desemnată, misiunea, competențele și responsabilitățile acestora fiind definite în mod oficial într-un regulament și aprobate de Consiliu, în conformitate cu Standardele.

AUDITUL SISTEMELOR INFORMATICE

Auditul sistemului informatic este o ramură a auditului general care se ocupă de controlul tehnologiilor informațiilor și comunicațiilor; studiază, în primul rând, sistemele și rețelele de calcul din punct de vedere al examinării eficienței controlului tehnic și procedural pentru a minimiza riscurile. Auditarea sistemului informatic presupune discuții cu personalul care stabilește specificațiile, dezvoltă, testează, conduce, administrează și utilizează sistemele de calcul.

Auditul sistemelor informatice reprezintă activitatea de colectare și evaluare a unor probe pentru a determina dacă sistemul informatic este securizat, menține integritatea datelor prelucrate și stocate, permite atingerea obiectivelor strategice ale întreprinderii și utilizează eficient resursele informaționale.

Auditul informatic reprezintă o formă esențială prin care se verifică dacă un sistem informatic își atinge obiectivul pentru care a fost elaborat. Standardele europene definesc clar domeniul, activitățile, etapele, conținutul auditării și formele de finalizare. Respectând cerințele acestora, rezultatul procesului de auditare informatică este eliberat de riscurile contestării. Auditul informatic reprezintă un domeniu cuprinzător în care sunt incluse toate activitățile de auditare pentru : specificații, proiecte, software, baze de date, procesele specifice ciclului de viață ale unui program, ale unei aplicații informatice, ale unui sistem

¹ Academia Comercială Satu Mare, lilianatodor@yahoo.com

informatic pentru management și ale unui portal de maximă complexitate, asociat unei organizații virtuale.

Potrivit standardelor, obiectul auditului sistemelor informatice poate fi focalizat pe programe, proiecte, sisteme informatice sau resurse informatice create sau utilizate în instituțiile private. Acestea pot fi auditate la nivel strategic, operațional sau la nivel de aplicație. Auditarea se poate desfășura pe întreg ciclul de viață al sistemului sau numai pe anumite etape: proiectare, dezvoltare, implementare, producție, livrare, interoperabilitate, acces, utilizare. Auditarea include, de asemenea, și evaluarea conformității cu legislația în vigoare. În cadrul misiunilor de audit al sistemelor informatice se va efectua evaluarea componentei aferente controalelor IT implementate în sistemul de control intern al entității auditate. Constatările vor evidenția punctele tari și punctele slabe ale sistemului informatic și vor menționa aspectele care trebuie remediate. Pe baza acestora se vor formula recomandări privind perfecționarea structurii de procese, controale și proceduri IT existente.

Principalele constatări, concluzii și recomandări formulate pe parcursul misiunii de audit vor fi sintetizate și vor fi înaintate conducerii entității auditate, constituind obiectul valorificării raportului de audit. Modul de implementare a recomandărilor și stadiul implementării acestora vor fi revizuite periodic, la termene comunicate entității auditate.

Se pot desfășura următoarele tipuri de audit IT:

- Evaluarea unui sistem informatic în scopul furnizării unei asigurări rezonabile privind funcționarea acestuia, asigurare necesară inclusiv misiunilor de audit financiar sau de audit al performanței la care este supusă entitatea;
- Evaluarea performanței implementării și utilizării sistemelor informatice;
- Misiuni de audit mixte, prin integrarea celor trei tipuri de audit: auditul financiar, auditul performanței și auditul IT, acestea urmând a se desfășura în cadrul unor misiuni comune, în funcție de obiectivele stabilite;

Evaluarea unui sistem IT integrat și/sau a unor aplicații individuale utilizate ca suport pentru asistarea deciziei (sisteme IT utilizate pentru evidență, prelucrarea și obținerea de rezultate, situații operative și sintetice la toate nivelele de raportare) în cadrul entității auditate. Extinderea utilizării tehnologiei informației în toate domeniile, inclusiv în cel al sistemelor financiar-contabile, care presupune atât extinderea controalelor IT în cadrul sistemului de control intern al entității auditate, generează necesitatea perfecționării modelelor tradiționale de auditare și extinderea auditului sistemelor informatice în activitatea unității.

Misiunea de audit al sistemelor informatice are în vedere următoarele criterii de evaluare generice:

- dacă sistemul informatic asigură un cadru adecvat, bazat pe integrarea tehnologiilor informatice pentru desfășurarea continuă a activității;
- dacă activitățile desfășurate pe parcursul derulării proiectelor IT sunt conforme cu obiectivele și termenele de realizare, aprobate la nivel instituțional, la fundamentarea acestora;
- dacă pe parcursul proiectelor s-au înregistrat dificultăți tehnice, de implementare sau de altă natură;
- dacă implementarea proiectelor conduce la modernizarea activității entității, contribuind la integrarea unor noi metode de lucru, adecvate și conforme cu noile abordări pe plan european și internațional
- dacă soluția tehnică este fiabilă și susține funcționalitatea cerută în vederea creșterii calității activității;
- dacă sistemul informatic funcționează în conformitate cu cerințele programelor și proiectelor informatice privind integralitatea, acuratețea și veridicitatea, precum și cu standardele specifice de securitate;

- dacă pregătirea utilizatorilor atinge nivelul performanței cerute de această nouă abordare, analizată prin prisma impactului cu noile tehnologii;
- dacă există și au fost respectate standarde privind calitatea suportului tehnic și metodologic.

Aceste criterii vor fi utilizate pe parcursul misiunii de audit IT, din perspectiva creării, la nivelul unității auditate, a unor arhitecturi de sistem coerente, bazate pe creșterea partajării informației și a sistemelor în administrație, reducerea costurilor totale prin reutilizare și evitarea duplicării aplicațiilor și sistemelor, reducerea timpului de implementare a proiectelor, îmbunătățirea manierei de administrare a proiectelor și de implementare a soluțiilor (portofoliul de proiecte), stabilirea politicilor de migrare pentru proiectele existente. Criteriile de audit pot fi diferite de la un audit la altul, în funcție de obiectivele specifice ale misiunii de audit.

ETAPELE AUDITULUI SISTEMELOR INFORMATICE

Etapele auditului sistemelor informatice sunt:

- planificarea auditului,
- efectuarea auditului,
- raportarea
- revizuirea auditului.

Planificarea este prima etapă din ciclul de viață al auditului, corectitudinea acesteia asigurând eficiența și execuția efectivă a tuturor celorlalte etape ale auditului. Presupune obținerea de informații privind entitatea auditată și de informații despre sistemul de control intern al acesteia. De asemenea, și foarte important, planificarea trebuie să includă o evaluare a riscurilor care decurg din funcționarea acestor sisteme. Planificarea auditului are la bază o strategie de audit, care se formulează pornind de la definirea abordării auditului și precizează elemente legate de coordonarea misiunii de audit, echipa implicată în această misiune, atribuțiile în cadrul echipei, orizontul de timp și direcțiile principale de acțiune. Scopul planificării auditului IT este acela de a obține o înțelegere a mediului în care funcționează sistemul informatic în cadrul entității auditate, de a evalua riscul de eroare sau de fraudă, de a elabora o abordare eficientă a auditului prin care să se colecteze probe suficiente și de încredere în scopul formării unei opinii, și de a alocă resursele necesare pentru realizarea acestor activități. Planificarea activităților are în vedere minimizarea costurilor auditului. Planificarea auditului sistemelor informatice trebuie să includă toate fazele necesare atingerii obiectivelor misiunii auditului, respectiv: documentarea privind activitatea auditată, programul sau sistemul care face obiectul auditului, stabilirea strategiei de audit, stabilirea procedurilor de audit și a tehnicilor aferente, a metodelor de sintetizare, analiză și interpretare a probelor de audit, identificarea și evaluarea riscurilor generate de furnizarea serviciilor electronice.

Evaluarea riscurilor

- după obținerea unei înțelegeri asupra mediului informatizat al entității, auditorul va evalua riscul inerent și riscul de control, factori care se iau în considerare la determinarea riscului de audit. Riscul de audit, indus de utilizarea sistemului informatic, poate fi exprimat în termenii următoarelor trei componente:

riscul inerent, care decurge din susceptibilitatea asupra resurselor informatice sau asupra resurselor controlate de sistemul informatic: furt material, distrugere, dezvăluire, modificări neautorizate, incompatibilitate, în lipsa controalelor interne asociate.

riscul de control, care reprezintă riscul ca erorile materiale din datele entității să nu fie prevenite sau detectate și corectate în timp util de structura controlului intern al entității.

riscul de nedetectare, care reprezintă riscul ca auditorul să nu detecteze erorile existente în sistem. Factori care afectează riscul inerent Operațiile informatizate pot introduce factori

adiționali de risc inerent. Auditorul trebuie să ia în considerare acești factori și să evalueze impactul prelucrărilor pe calculator asupra riscului inerent. Pentru sistemele informatice financiar-contabile, cei mai relevanți factori induși de mediul informatizat sunt menționați în continuare.

Prelucrarea uniformă a tranzacțiilor: favorizează propagarea erorilor pentru tranzacțiile similare și reduce substanțial posibilitatea prelucrării selective a erorilor.

Prelucrarea automată: probele aferente acestor operațiuni pot sau nu pot fi vizibile.

Potențial crescut de nedetectare a greșelilor: se datorează implicării umane în prelucrare mai puțin decât în sistemele manuale, ceea ce crește potențialul obținerii accesului neautorizat al indivizilor la informațiile sensibile și al alterării datelor fără probe vizibile. Datorită formatului electronic, schimbările programelor și datelor sunt dificil de detectat. De asemenea, este probabil ca utilizatorii să poată interveni mai ușor asupra formei electronice decât asupra rapoartelor manuale.

Existența, completitudinea și volumul parcursului auditului: parcursul auditului financiar reprezintă proba care demonstrează modul în care a fost inițiată, prelucrată și agregată o tranzacție specifică și reprezintă o cerință fundamentală. Anumite sisteme informatice sunt proiectate pentru a reține parcursul auditului numai pentru o perioadă scurtă, numai în format electronic și numai într-o formă sintetică. De asemenea, informația generată poate fi prea voluminoasă pentru a putea fi analizată cu eficacitate. Tranzacțiile pot rezulta dintr-o agregare a informației din numeroase surse. Fără utilizarea unor produse software de regăsire și prelucrare, extragerea tranzacțiilor ar putea deveni extrem de dificilă. Fără un parcurs al auditului, poate să nu fie fezabilă formularea unei opinii categorice privind situațiile financiare. Sistemele financiare trebuie să permită auditorului să urmărească tranzacțiile începând cu intrarea inițială, tranzacțiile generate de sistem și tranzacțiile cu alocare internă; până la reflectarea lor corectă în situațiile financiare. Toate datele relevante și informațiile de parcurs al auditului financiar trebuie reținute un timp suficient pentru finalizarea auditului. Documentele sursă trebuie de asemenea să facă parte din parcursul auditului financiar, și acestea trebuie și ele să fie păstrate până la finalizarea auditului.

Natura configurației hardware și software utilizate: tipul de prelucrare (locală, online, distribuită); dispozitivele periferice, interfețele sistem sau conexiunea la Internet; rețelele distribuite, furnizarea serviciilor IT. Riscurile tipice sunt: accesul neautorizat la resursele sistemului, posibila alterare a datelor, dezvăluirea informațiilor sensibile, dependența de furnizorul de programe.

Riscurile generice asociate sistemului informatic, detectate pe parcursul unei misiuni de audit al sistemelor informatice vor fi clasificate în trei categorii:

a) Riscuri privind planificarea, dezvoltarea și introducerea sistemelor și serviciilor informatice

Aceste riscuri decurg din:

- Lipsa unei planificări strategice;
- Insatisfacția utilizatorilor; ignorarea explorării profilului utilizatorilor;
- Neglijarea aspectelor legate de asigurarea calității;
- Lipsa unor evaluări privind eficacitatea costurilor;
- Neîndeplinirea atribuțiilor privind crearea cadrului necesar legal și organizațional;
- Implicarea sporadică și inconsecventă în elaborarea și implementarea reglementărilor și standardelor IT și de securitate;
- Furnizarea neadecvată a infrastructurii tehnice;
- Dependența de companiile IT;
- Lipsa reglementării drepturilor privind rețeaua Internet;
- Lipsa unor evaluări ale proiectelor raportate la evoluțiile tehnologiilor informației și comunicațiilor

b) Riscuri în funcționarea sistemelor și serviciilor informatice

Aceste riscuri decurg din:

Politici de securitate IT tehnică și organizațională neadecvate, care afectează integritatea, autenticitatea, confidențialitatea și disponibilitatea informațiilor; securizarea transferului de date;

Capabilitățile de auditare a informațiilor; Securitatea tranzacțiilor;

Redundanță, discontinuități media și interoperabilitate neadecvată.

c) Riscuri și efecte în plan economic

Aceste riscuri decurg din:

Decizii neadecvate, datorate pierderilor sau alterării informațiilor furnizate de sistemul informatic;

Pierderi datorate unor disfuncționalități generate de indisponibilitatea informațiilor în timp real;

Dezvoltarea și implementarea necontrolată a unor componente informatice eterogene;

Cheltuieli dispersate, nejustificate;

Scăderea eficienței serviciilor informatice furnizate.

Planul de audit conține următoarele secțiuni:

1. *Informații despre entitatea auditată:* obiective, structură, dotare hardware și software, volumul operațiilor prelucrate automat;

2. *Stabilirea obiectivelor auditului:* abordarea auditului, aria de acoperire a auditului, rolul auditorului IT;

3. *Evidențierea domeniilor critice care vor fi examinate:* ariile cu riscul cel mai ridicat;

4. *Criteriile de audit stabilite;*

5. *Etapile misiunii de audit și tipurile de evaluări aferente:* procedurile de audit prin care se

obțin probele de audit, metodele și tehnicile de analiză, sinteză și interpretare a probelor de audit;

6. *Resurse necesare:* personal, timp, resurse tehnice și financiare.

Probele de audit specifice sistemelor informatice pot fi încadrate în următoarele categorii:

a) *Probe de audit fizice* - rezultate din demonstrații ale aplicațiilor, documentații tehnice, diagrame, scheme de arhitectură și alte elemente echivalente acestora.

b) *Probe de audit verbale* – răspunsuri la interviuri, sondaje.

c) *Probe de audit documentare* – documente, documentații, manuale în formă scrisă sau în format electronic.

d) *Probe de audit analitice* – rezultate obținute în urma evaluărilor și analizei fondului de informații(indicatori,tendințe)

STANDARDELE INTERNAȚIONALE PENTRU PRACTICA PROFESIONALĂ A AUDITULUI INTERN

Auditul intern este o activitate independentă de asigurare obiectivă și de consiliere, destinată să adauge valoare și să antreneze îmbunătățirea activităților organizației, pe care o susține în îndeplinirea obiectivelor sale. Ajută organizația în îndeplinirea obiectivelor sale printr-o abordare sistematică și disciplinată în cadrul evaluării și îmbunătățirii eficacității proceselor de management al riscurilor, control și guvernare.

Activitățile de audit intern se desfășoară în diferite medii legislative și culturale; în cadrul unor organizații care diferă din punct de vedere al scopului, mărimii, complexității și structurii; de către persoane din cadrul sau din afara organizației. Deși pot exista diferențe privind practica auditului intern în fiecare dintre aceste medii, este esențial să se respecte Standardele Internaționale pentru Practica Profesională a Auditului

Intern, pentru ca responsabilitățile auditorilor interni să fie îndeplinite. Dacă auditorii interni sunt îngrădiți de legislație sau regulamente și, drept urmare, nu pot respecta anumite părți ale Standardelor, ei trebuie să respecte toate celelalte secțiuni ale Standardelor și să declare neconformitatea produsă. Misiunile de asigurare implică evaluarea obiectivă a probelor de către auditorul intern, în vederea formulării unei opinii independente sau a unor concluzii privind un proces, sistem sau alt subiect supus auditului. Tipul și sfera de cuprindere a misiunilor de asigurare sunt stabilite de către auditorul intern. În general, sunt implicate trei entități în misiunile de asigurare: (1) persoana sau grupul implicat(ă) direct în procesul, sistemul sau subiectul auditat – responsabilul pentru proces, (2) persoana sau grupul care efectuează evaluarea – auditorul intern, (3) persoana sau grupul care utilizează rezultatul evaluării – beneficiarul misiunii.

Misiunile de consiliere au un caracter consultativ și se desfășoară în general la cererea expresă a beneficiarului misiunii. Tipul și sfera de cuprindere a serviciilor de consiliere sunt stabilite de comun acord cu beneficiarul misiunii. Misiunile de consiliere implică în general două entități:

- (1) persoana sau grupul care oferă consiliere – auditorul intern și
- (2) persoana sau grupul care solicită și primește consiliere – beneficiarul misiunii. În îndeplinirea misiunilor de consiliere, auditorul intern trebuie să își păstreze obiectivitatea și să nu își asume responsabilitatea conducerii.

Scopul *Standardelor* este:

1. Să contureze principiile de bază care reprezintă practica de audit intern așa cum trebuie ea să fie.
2. Să furnizeze un cadru general de realizare și susținere a unei game largi de activități de audit intern care generează o valoare adăugată.
3. Să funcționeze ca un cadru de referință pe baza căruia se evaluează rezultatele auditului intern.
4. Să stimuleze îmbunătățirea proceselor și operațiunilor organizației.

Există un singur set de Standarde de Calificare și de Performanță, însă sunt mai multe seturi de Standarde de Implementare: câte un set pentru fiecare tip principal de activitate de audit intern. Standardele de Implementare au fost stabilite pentru activități de asigurare (A) și de consiliere (C).

Standardele fac parte din Cadrul General al Practicii Profesionale. Cadrul General al Practicii Profesionale include Definiția Auditului intern, Codul de etică, Standardele și alte îndrumări. Îndrumări privind modul în care pot fi aplicate Standardele sunt incluse în Modalități practice de aplicare, care sunt redactate de Comitetul de rezolvare a problemelor profesionale.

Standardele folosesc o terminologie specifică, sensul termenilor fiind explicat în Glosar.

Îmbunătățirea și publicarea Standardelor este un proces continuu. Consiliul de Standardizare a Auditului Intern poartă consultări și discuții ample înainte de publicarea Standardelor. Acestea includ solicitări către publicul din întreaga lume de a trimite puncte de vedere cu privire la proiectul de standarde în dezbatere.

CONCLUZII

Îndeplinirea misiunii de audit implică parcurgerea procedurilor și documentelor specifice structurate pe cele patru etape prezentate prin normele generale.

- În etapa de pregătire a misiunii de audit intern s-au elaborat documentele

prevăzute de normele generale aducându-se clarificări, mai ales cu privire la modul de dezvoltare a *Analizei riscurilor*, succesiunea documentelor, structura și modul de completare al acestora, nivelul de apreciere și împărțire al riscurilor, clasarea și ierarhizarea lor în scopul finalizării procedurii pe baza căreia se va concentra *Programul intervenției a fața locului*.

- În următoarea etapă s-au realizat testarea pe teren a operațiilor auditabile, pe baza Programului intervenției la fața locului, prin utilizarea diferitelor tehnici de eșantionare, liste de verificare, teste, foi de lucru, interviuri și note de relații, elemente care s-au constituit în probe de audit și au stat la baza întocmirii FIAP-urilor și FCRI-urilor, care vor fi incluse în raport.

- În etapa de elaborare a Raportului de audit intern se urmărește o structurare a acestuia pe Tematica în detaliu a misiunii de audit care este obținută în procedura de Analiza riscurilor și transferarea FIAP-urilor și FCRI-urilor într-o manieră standardizată astfel încât să poată fi utilizat de factorii de management.

- În etapa de urmărire a recomandărilor în afara documentelor stabilite de normele generale au fost recomandate câteva modele de documente pentru evaluarea internă și externă a activității de audit intern.

BIBLIOGRAFIE

Ghiță, M., Briciu, S. și colab., 2005, Audit intern, Ed. ULISE, Alba Iulia

Ghiță, M., Sprânceană, M., 2006, Auditul intern în sistemul public, Ed. Tribuna Economică, București

Ghiță, M., Pop, R., Ghiță, R., Timar, Alina, 2011, Guvernanța corporativă și auditul intern, Ed. Casa Cărții de Știință, Cluj-Napoca

- ❖ Legea nr.672/2002
- ❖ OG nr. 37/2004 și aprobată de Legea 106/2004
- ❖ Ordinul Ministerului Finanțelor Publice nr. 38/2003 modificat și completat prin Ordinul Ministerului Finanțelor Publice nr. 423/2004 pentru aprobarea Normelor generale de exercitare a auditului public intern
- ❖ Normelor metodologice proprii ale SNLO cu privire la Auditul Intern
- ❖ Partea I din Normele generale de exercitare a auditului public intern, aprobate prin OMFP nr. 38/2003