

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 aloca 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

