

Capitolul 4

CONTROLUL APLICATIILOR

CONTROLUL GENERAL – CONTROLUL APLICATIILOR

- Controlul general asigura integritatea sistemului vazut ca un intreg, inclusiv executia aplicatiilor si controlul fisierelor exploatate.
- Controlul aplicatiilor asigura acuratetea, integritatea si completitudinea tranzactiilor.

CONTROLUL APLICATIILOR

- Obiectivele controlului raman aceleasi
- Controalele derulate pot fi manuale sau automate.

1. TIPURI DE CONTROALE

- Controlul datelor de intrare
- Controlul prelucrarilor
- Controlul integritatii fisierelor
- Controlul securitatii aplicatiei
- Controlul iesirilor
- Controlul fisierelor principale (MASTER FILES)

2. UTILIZATORII APLICATIEI

- proprietarul
- administratorul
- utilizatori curenti

- PROPRIETARUL

- utilizator principal
- are responsabilitatea aplicatiei
- nu este implicat in executarea aplicatiei
- deleaga sarcini

- ADMINISTRATORUL

SARCINI:

- sa asigure functionarea controlului logic asa cum s-a prevazut
- sa asigure actualizarea controlului logic
- sa verifice existenta backup-ului aplicatiei
- sa rezolve cerintele utilizatorilor
- sa asigure identificarea, monitorizarea si raportarea problemelor
- pastrarea si distributia documentatiei
- asigura legatura intre departamentul IT, utilizatorii sistemului si firma software furnizoare.

- **UTILIZATORII CURENTI**

- Aplicatia reprezinta un instrument de lucru pentru realizarea sarcinilor lor
- Sunt instruiti cum sa foloseasca aplicatia pentru a-si realiza sarcinile de serviciu.

3. CLASIFICAREA APLICATIILOR

- Sisteme cu intrari de tip batch (loturi)
- Sisteme cu intrari de tip batch si consultare online
- Sisteme cu procesare pe loturi si consultare online

4. AUDITOR – CONTROLUL APLICATIEI

- Auditorul trebuie sa dopte o abordare eficienta si eficace a auditului
- Auditorul trebuie sa cunoasca si sa inteleaga sistemul si controalele interne
- Daca controalele acopera obiectivele auditului si par a fi robuste auditorul poate selecta testele considerate ca necesare.

5. PLANUL DE AUDIT

Contine :

- obiectivele fixate
- probele pe care auditorul se asteapta sa le obtina in urma auditului
- amploarea (intinderea) testelor programate
- ce se va considera ca esec al controlului
- cate astfel de esecuri pot fi tolerate

6. PROBELE

- Probele pot fi sub forma :
 - Listelor de control al accesului
 - Limitelor autorizarilor automate ale utilizatorilor
 - Jurnalului de securitate
 - Cererile de modificari si modul de solutionare a acestora etc.
- Se obtin prin combinarea :
 - Observarii
 - Chestionarii
 - Examinarii
 - Esantionare (folosind tehnici asistate de calculator)

7. CAT DE DEPARTE SA SE MEARGA CU TESTELE?

- Rationamentul auditorului
- Rationamentul ia in considerare:
 - Frecventa controlului
 - Gradul de incredere prezentat de controalele aplicatiei
 - Natura probelor pe care auditorul urmareste sa le obtina
 - Continuitatea controlului
 - Importanta controlului si a tranzactiilor.

CONTROLUL INTRARILOR, PRELUCRARI LOR SI IESIRILOR

LA CE FOLOSESC CONTROALELE APLICATIEI?

- Asigura completitudinea, acuratetea si validitatea inregistrarilor
- Controalele vizeaza : intrarile, prelucrarile, iesirile.

RESPONSABILITATI

- Cine are responsabilitatea acestor controale?
- Sunt cele mai adecvate controale ?
- Ce rol are auditorul IT?

INTELEGHEREA SI DOCUMENTAREA PRIVIND APLICATIILE FINANCIARE

- Auditorul trebuie sa produca dovezi ca a inteles modul de functionare a SI si controalele acestuia
- Aceasta a obtinut cunoasterea si prin documentare asupra :
 - Fluxului tranzactiilor prin sistem
 - Controalele aplicate intrarilor, prelucrarilor, iesirilor.
- Auditorul trebuie sa identifice si sa cunoasca orice documentatie a aplicatiei existenta la client.

CONTROLUL INTRARILOR

- Este folosit pentru a asigura ca toate tranzactiile sunt :
 - introduse corect
 - complete
 - valide
 - autorizate
 - aferente perioadei de gestiune curente
 - inregistrate corect in conturi (in cazul aplicatiilor contabile).

AUTORIZAREA

- Autorizarea controalelor reduce riscul erorilor, fraudei si tranzactiilor ilegale
- Autorizarea poate fi controlata prin identificarea utilizatorului, care a introdus datele in sistem, pe baza privilegiilor asociate ID-urilor utilizatorilor
- Se introduc doar date autorizate? Cine si cum autorizeaza datele de intrare?

- Validarea intrarilor

- se poate realiza manual sau automat
- controalele de validare trebuie sa asigure indeplinirea criteriilor de validare a datelor stabilite
- reduce riscul introducerii de date incorecte

- Maxima "garbage in – garbage out" atentioneaza asupra importantei acuratetei datelor de intrare. Este mai eficient sa aloca resurse pentru

asigurarea acuratetei si completitudinii datelor de intrare decat sa fii nevoit sa le corectezi in timpul sau, mai grav, dupa incheierea procesului de prelucrare si chiar a depunerii situatiilor financiare.

- Controlul datelor de intrare trebuie adaptat la modalitatile diferite de introducere a datelor in sistem :
 - de la tastatura (unde riscul erorilor este mai mare)
 - scanarea documentelor
 - utilizarea perifericelor senzoriale
 - citirea barelor de cod
 - ATM-uri si terminale POS
 - EDI (ELECTRONIC DATA INTERCHANGE)
 - generarea automata a tranzactiilor (ex. : plati planificate, calcularea lunara a dobanzilor)

⇒ Nu toate intrarile prezinta un suport material (documente pe suport hartie), multe fiind in format electronic.

⇒ In cazul preluarii automate sau generarii automate exista riscuri mai mici de eroare fata de preluarea datelor prin tastare.

- Tipuri de controale aplicate asupra datelor de intrare

CONTROLUL FORMATULUI

- Se verifica :

- Natura datelor
- Lungimea datelor → trunchieri
- Numarul de zecimale admis
- Acceptarea valorilor negative sau doar a celor pozitive
- Formatul datei calendaristice
- Aplicarea semnului monetar

CONTROLUL DOMENIULUI DE DEFINITIE A ATRIBUTELOR

a) incadrarea intr-o multime de valori prestabilita (ex.: abrevierile judetelor, tipuri de unitati de masura, tipuri de documente)

b) incadrarea intr-un interval de valori prestabilit (ex.: salariul angajatilor ia valori in intervalul [2.500.000, 30.000.000])

c) validari ale realizarilor unor atribute diferite numit si testul dependentei logice dintre campuri. Ex.: validările privind corespondenta conturilor – contul X se poate debita doar prin creditarea conturilor A,B,C.

d) testul “rezonabilitatii” datelor :

- aceste teste verifica daca datele sunt rezonabile in raport cu un standard sau date introduse anterior. Datele standard pot fi stocate intr-un fisier sau pot reprezenta constante definite la nivelul aplicatiei (ex.: un standard poate fi reprezentat de numarul de ore lucratoare intr-o luna, stabilit in functie de zilele lucratoare si sarbatorile legale, nivelurile de dobanda practicate de banca etc.)

CONTROLUL ACURATETEI ARITMETICE

- Pe baza unor date de intrare introduse de operator pot fi verificate elementele calculate din documentul primar

Ex. : pe baza cantitatii si pretului unitar al unui articol in scris intr-o factura sistemul genereaza automat pe ecran valoarea produsului, TVA-ului, valoarea cu TVA si apoi totalul facturii operatorul putand confrunta aceste sume calculate cu cele inscrise in factura.

CONTROLUL EXISTENTEI DATELOR

- Testul se refera in principal la validarea datelor de intrare reprezentand coduri. Este suficient sa introduci codul unui client si pe ecran sa se afiseze numele acestuia sau un mesaj de eroare atentionand asupra introducerii unui cod incorect.

TESTUL CIFREI DE CONTROL

- se aplica asupra datelor de intrare reprezentand elemente codificate
- urmareste rejectarea codurilor eronate introduse
- cauza erorii la nivelul elementelor codificate poate fi :
 - Trunchierea
 - Adaugarea unui caracter suplimentar
 - Transcrierea incorecta a codului in documentul primar
 - Transpozitia caracterelor la introducerea codului.
- presupune determinarea cifrei de control aferente codului introdus prin aplicarea algoritmului prestabilit. In masura in care cifra de control determinata automat nu corespunde celei incluse in codul introdus sistemul va trebui sa atentioneze printr-un mesaj corespunzator asupra erorii aparute.

TESTUL TRANZACTIILOR DUPLICATE

- sistemul admite introducerea repetata a acelorasi date?
Ex. : introducerea repetata a unui aceluasi document (factura, bon de consum etc.).

SOLUȚIONAREA TRANZACTIILOR REJECTATE

- cum se solutioneaza tranzactiile neacceptate de sistem (care nu au trecut testul de validare)?
- cine raspunde de verificarea acestor date de intrare si de reintroducere lor?
- sunt generate liste continand intrarile rejectate?
- daca aceste tranzactii sunt consemnate in documentele primare depistarea erorii este mai usoara si corectarea se poate face fara probleme deosebite. Probleme particulare apar in cazul tranzactiilor online.

CONTROLUL PRELUCRARI LOR

Auditorul tine seama de:

- Tipologia sistemului informatic:

- Sisteme de procesare a tranzactiilor (TPS – Transaction Processing Systems)
- Sisteme destinate conducerii curente (MIS – Management Information Systems)
- Sisteme suport de decizie (DSS – Decision Support Systems)
- Sisteme destinate conducerii strategice (EIS – Executive Support Systems)
- Sisteme pentru automatizarea lucrarilor de birou (OAS – Office Automation Systems)
- Modalitatilor de introducere a datelor in sistem si procesarea acestora:
 - Introducere pe loturi – procesare pe loturi
 - Introducere on line – procesare pe loturi
- Natura prelucrarilor:

In cadrul TPS-urilor, de exemplu, pot fi identificate proceduri de:

 - Actualizare a bazei de date
 - Sortare
 - Calcul
 - Consultare
 - Salvare si restaurare a bazei de date etc.
- Nivelul de descentralizare a prelucrarilor.

Controlul fisierelor si al bazei de date

Se verifica:

- Continuitatea acestora
- Versiunea – Este ultima versiune? Cuprinde ea toate corectiile?
- Transferul fisierelor in momentul trecerii la exploatarea unui nou sistem informatic. Se verifica masura in care au fost autorizate procedurile de transfer al fisierelor din vechiul in noul sistem. Au fost aceste proceduri realizate de persoanele imputernicite? Se verifica completitudinea si corectitudinea transferului.
- Solutia aleasa pentru arhitectura bazei de date este cea mai buna (variantele baza de date centralizata sau baza de date distribuita)?
- In cazul bazelor de date distribuite s-a realizat o corecta si eficienta distribuire a datelor in nodurile retelei? In ce masura s-a tinut seama de respectarea urmatoarelor cerinte:
 - ◆ Nevoile de informare a utilizatorilor locali
 - ◆ Asigurarea unui transfer minim al datelor prin retea
 - ◆ Necesitatea protectiei datelor transferate prin retea.
- Care au fost criteriile pentru alegerea SGBD-ului? Ofera SGBD-ul toate facilitatile privind implementarea controalelor automate, al controlului accesului la baza de date, tabelele bazei de date etc.

Disponibilitatea datelor

Datele, in procesul prelucrarii, datorita reprezentarii binare sunt inaccesibile auditorului in aceasta forma. Mai mult, unele date sunt temporar stocate in memoria calculatorului (datele intermediare de lucru).

Controlul prelucrarilor declansate automat

- Auditorul trebuie sa verifice care sunt evenimentele care declanseaza aceste prelucrari;
- Controlul tranzactiilor generate automat.

Functionalitatea aplicatiei

- Exista anumite prelucrari pe care aplicatia trebuie sa le execute, dar nu le realizeaza sau le realizeaza greoi?

- Sunt functionalitati care lipsesc?
- In ce masura aplicatia raspunde stilului si metodei de lucru specifice utilizatorului?
- Determina aplicatia un mod de lucru ineficient, o gandire rigida, nenaturala?

Controlul fluxului prelucrarilor

- Presupune sa verificam ce prelucrari urmeaza sa se declanseze in anumite circumstante.
- Testul *load conditions* : un program poate functiona nesatisfacator cand este suprasolicitat (volum mare de date de prelucrat intr-un interval scurt de timp sau incarcare maxima intr-un anumit moment).

Comunicarea sistemului cu utilizatorul

- Este usor "sa te pierzi" in program?
- Exista optiuni de lucru care pot fi confundate cu altele?
- Care sunt mesajele de eroare? Sunt utile, explicite?
- Ce informatie este disponibila pe ecran? Este suficienta, clara?
- Calitatea asistentei oferite utilizatorului (informatia returnata de tasta HELP de exemplu).

Performante

In cazul sistemelor in timp real este foarte important timpul de raspuns.

Integrarea prelucrarilor

CONTROLUL DATELOR DE IESIRE

Urmareste :

- Completitudinea si acuratetea iesirilor
- Respectarea termenelor prevazute pentru obtinerea iesirilor
- Masura in care iesirile, la cererea utilizatorilor, pot fi dirijate catre imprimanta, monitor sau un fisier.
- Distribuirea iesirilor catre persoanele autorizate :
 - Cine primeste situatiile? Exista persoane imputernicite in acest sens?
 - Situatiile continand date sensibile sunt preluate pe baza de semnatura?
 - Cum este asigurata protectia informatiilor confidentiale?
- Iesirile catre alte aplicatii se realizeaza in formatul pe care acestea il necesita?
- Masura in care se realizeaza inregistrarea, raportarea si corectarea erorilor identificate.
- In ce masura exista din partea managementului un control asupra acuratetei iesirilor si modului de distribuire a lor.

CONTROLUL SECURITATI I APLICATIEI

Controalele securitatii aplicatiei sunt folosite pentru asigurarea :

- Integritatii tranzactiilor si fisierelor;
- Acuratetei prelucrarilor;
- Separarii sarcinilor incompatibile intre persoanele implicate in procesarea datelor;
- Controlul utilizatorilor.

Modalitati de realizare a controlului securitatii aplicatiei:

- Identificarea si autorizarea utilizatorilor
- Controlul accesului
- Monitorizarea activitatii utilizatorilor.

1. Identificarea si autorizarea utilizatorilor

Se realizeaza prin controlul jurnalelor aplicatiei :

- Jurnalul ID-urilor si parolelor utilizatorilor: auditorul trebuie sa evalueze politicile de securitate ale aplicatiei si procedurilor din cadrul acesteia.
- Controalele jurnalelor variaza de la o aplicatie la alta (nu sunt aceleasi in toate aplicatiile).
- Este necesara revederea manualelor aplicatiei pentru cunoasterea controalelor plecand de la jurnalele generate de aplicatie.

2. Controlul accesului

Se verifica:

- Controlul accesului la aplicatie prin log-are
- Restrictionarea accesului la modulele aplicatiei
Exemplu: gestionarul poate sa incarce notele de receptie si constatare de diferente precum si bonurile de consum in modulul de gestiune dar nu poate avea acces la modulul de contabilitate sau cel de calcul al salariilor.
- Restrictionarea accesului la anumite functii ale aplicatiei.
- Existenta listelor de control al accesului.

3. Monitorizarea activitatii utilizatorilor

- Utilizatorii trebuie urmariti (controlati) cu privire la actiunile pe care le desfasoara.
- Monitorizarea actiunilor utilizatorilor asigura:
 - limitarea erorilor si fraudelor
 - identificarea utilizatorilor si actiunilor lor
 - responsabilitatea utilizatorilor pentru rezultatele obtinute.
- Monitorizarea actiunilor utilizatorilor se realizeaza prin intermediul jurnalelor.
- Auditorul poate culege probe deosebit de utile prin verificarea jurnalelor realizate de aplicatie. Auditorul are obligatia sa verifice modul in care este asigurata protectia acestor jurnale pentru ca probele obtinute pe baza lor sa fie credibile.

COLECTAREA SI EVALUAREA PROBELOR

Abordari:

- Orientate catre date
- Orientate catre sistem

Misiunea de audit impune, chiar daca predominant sunt desfasurate proceduri orientate catre date, si studierea sistemului informatic in ansamblul sau.

Abordarea orientata catre date

- Se pune accent pe testele datelor de iesire
- Daca acuratetea iesirilor, dovedita in urma testelor desfasurate de auditor, este satisfacatoare atunci exista si increderea asupra inregistrarilor si procesarilor din cadrul sistemului.

- Recomandata in cazul sistemelor informatice avand o arie restransa si o complexitate redusa.

Abordarea orientata catre sistem

- Auditorul isi focalizeaza atentia asupra sistemului informatic in ansamblul sau: testele asupra controalelor preventive si corective precum si asupra prelucrarilor si securitatii sistemului pot constitui probe pentru auditor ca rezultatele generate de sistem sunt corecte.

Raman valabile prevederile Standardului de audit 500 – Probe de audit:

- Necesitatea unor probe de audit adecvate si suficiente

Suficienta indica masura cantitatii probelor de audit.

Gradul de adecvare indica masura calitatii probelor si a relevantei lor.

- Rationamentul auditorului privitor la ce inseamna o proba de audit adecvata si suficienta precum si factorii de influenta asupra rationamentului.

Controalele

- Auditorul in urma documentarii desfasurate trebuie sa cunoasca si sa poata evalua controalele manuale si automate existente in sistem.
- Consistenta, acuratetea si continuitatea controalelor din sistem ofera auditorului certitudinea asupra acuratetei si completitudinii datelor, calitatii prelucrarilor ceea ce-l va ajuta la determinarea naturii, intinderii si complexitatii testelor pe care urmeaza sa le desfasoare.
- Complexitatea sistemelor informatice contabile impune necesitatea abordarii lor pe subsisteme. Pentru fiecare subsistem in parte, auditorul realizeaza diagrame ale fluxurilor de date pentru evidentiarea:
 - intrarilor
 - fisierelor utilizate
 - procesarilor
 - iesirilor

- controalele manuale si automate implementate evaluand masura in care sunt suficiente si acoperitoare. Auditorul va trebui sa raspunda la urmatoarele intrebari:

 - Care sunt controalele de baza?
 - Se suprapun, in unele cazuri, controalele manuale peste cele automate? Acest lucru creste gradul de incredere asupra controalelor.
 - Care sunt controalele interdependente din cadrul aplicatiei? Ex.: Creditul fixat pentru un credit card este controlat si in procedura de gestiune a tranzactiilor si trebuie sa fie acelasi cu cel retinut in fisierul CARDURI.

- verificarea procedurilor prin care sunt corectate erorile: auditorul trebuie sa aiba certitudinea ca aceste proceduri exista si functioneaza corect.

Eroare: inexactitate involuntara aparuta in situatiile financiare. Tipuri de erori:

 - erori de calcul
 - erori de inregistrare
 - erori de contare etc.

Ce poate fi considerata eroare semnificativa?
- Determinarea gradului de incredere al controalelor automate se realizeaza in urma desfasurarii:

- unor teste independente
- testarea controalelor existente in sistem.

Strategii ale auditului sistemelor informatice contabile

- Testele desfasurate ajuta sa formulam o opinie privitoare la acuratetea prelucrarilor din cadrul sistemului
- Strategiile de auditare pot fi clasificate astfel:
 - **Auditare cu ajutorul calculatorului**
 - **Auditare in afara calculatorului**
 - **Auditare prin calculator**

Auditarea cu ajutorul calculatorului

- Include testarea calculelor executate in timpul procesarii tranzactiilor, compararea datelor din fisiere diferite atunci cand datele respective ar trebui sa prezinte valori identice etc.
- Programul auditorului selecteaza esantionul de test pe baza unor variabile precizate de auditor, datele esantionului generand un fisier de lucru asupra caruia se aplica prelucrarile continute in programul auditorului, auditorului generandu-i-se un raport.
Un *esantion de test* reprezinta un set de tranzactii selectate aleator, concluziile desprinse din analiza acestora putand fi generalizate la nivelul tuturor tranzactiilor din sistem.

Auditarea in afara calculatorului

- Se pleaca de la tranzactiile de intrare ale perioadei auditate, prelucrarea acestora realizandu-se manual. Daca rezultatele obtinute sunt aceleasi cu cele generate de aplicatia auditata inseamna ca logica interna a aplicatiei produce rezultate corecte, acceptate de auditor.
- Avantaje:
 - Este usor de realizat
 - Nu impune costuri mari
 - Nu necesita cunostinte privind prelucrarea automata a datelor.
- Dezavantaje:
 - Calitatea opiniei formulate de auditor depinde de esantionul pe care s-a facut testul (rationamentul auditorului care a condus spre respectivul esantion). Esantionul poate sa nu cuprinda tranzactii capabile sa evidentieze erori de procesare si lipsa unor controale.
 - Priveste mai mult procesarile finalizate decat prevenirea problemelor legate de prelucrarea in viitor a datelor. Doar daca se identifica o eroare logica conduce la efecte pozitive privind procesarea datelor in viitor.
 - Se desfasoara manual si consuma mai mult timp.

Auditarea prin calculator

- Pleaca de la presupunerea ca anumite date, prelucrate printr-o anumita aplicatie, produc anumite iesiri.

- Foloseste teste care sa arate **cum** sunt prelucrate datele.
- Auditorul stabileste datele de test (deci nu se lucreaza cu date reale), simuland tranzactii care prin cazuistica lor pot evidentia eventualele carente ale controalelor si prelucrarilor urmarind sa verifice daca datele de test declanseaza controalele corespunzatoare. Auditorul compara rezultatele prelucrarii datelor de test prin sistemul auditat cu iesirile anticipate de el.
- Se pleaca de la ideea ca cea mai buna testare este cea realizata in conditii reale de exploatare.
- Au operatorii la dispozitie doar versiunea executabila a aplicatiei sau si programul sursa?
- Au programatorii acces doar la modulele in lucru (activitatea de dezvoltare a aplicatiilor) si de test ale aplicatiilor sau au acces si la aplicatia curenta aflata in exploatare?

Testele auditorului trebuie sa se efectueze fara a fi anuntate. Se evita astfel posibilitatea ca persoanele implicate in fraudare sa stearga urmele interventiei lor refacand fisierele si aducand aplicatia la versiunea corecta.

Testul lungimii aplicatiei (testul byte-count)

- Compara lungimea in bytes a aplicatiei aflata in exploatare cu backup-ul aplicatiei. Testul este elocvent pentru ca este imposibil sa realizezi modificari intr-un program fara ca lungimea acestuia sa nu se modifice.
- Eventualele diferente intre lungimile celor doua aplicatii determina identificarea cauzelor.

Testul logicii programului

- Se executa atunci cand auditorul are convingerea ca in program s-au facut modificari neautorizate.
- Copia de siguranta a aplicatiei se considera autentica si va constitui proba martor.
- Presupune executarea unui program care compara byte cu byte aplicatia aflata in exploatare cu backup-ul.

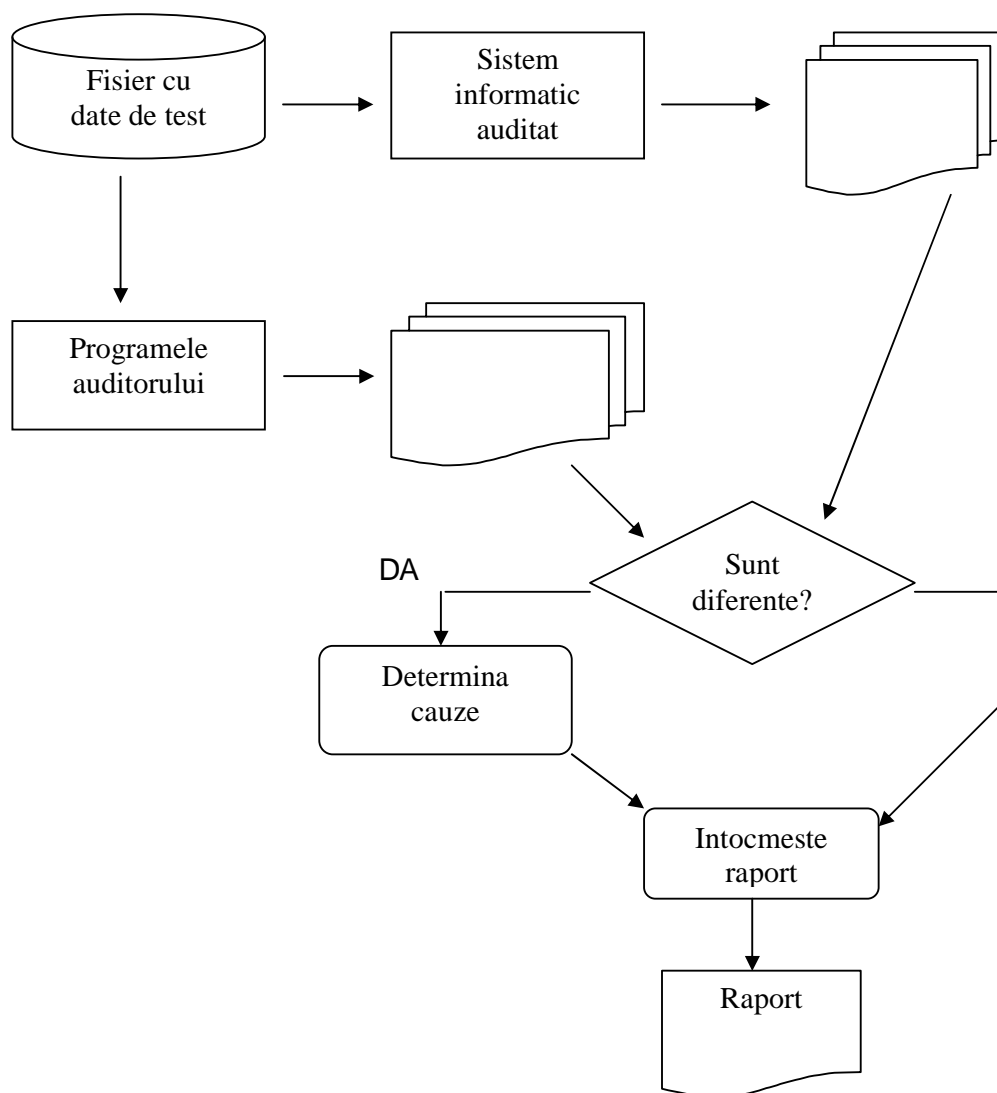
Ansamblul programelor folosite de auditor in realizarea misiunii sale se cuprind in conceptul generic de ***tehnici de audit asistate de calculator (CAAT)***.

Definirea, descrierea si prezentarea modului de utilizare a CAAT se gaseste in **Standardul de audit nr. 1009 – Tehnici de audit asistate de calculator**.

In conformitate cu acest standard:

- Software-ul pentru audit consta in programe utilizate de catre auditor, ca parte a procedurilor de audit, pentru a procesa date cu semnificatie pentru audit din sistemul contabil al firmei auditate.
- El poate consta din :
 - *Pachete de programe* – programe generalizate, proiectate sa efectueze functii de procesare a datelor ca de exemplu: citirea fisierelor, selectarea informatiilor, executarea calculelor, crearea fisierelor, tiparirea de rapoarte in structura ceruta de auditor.
 - *Programe realizate pentru un anumit scop* – programe realizate sa execute sarcini de audit in circumstante specifice. Pot fi elaborate de auditor, de specialistii firmei auditate sau de un informatician angajat de auditor.

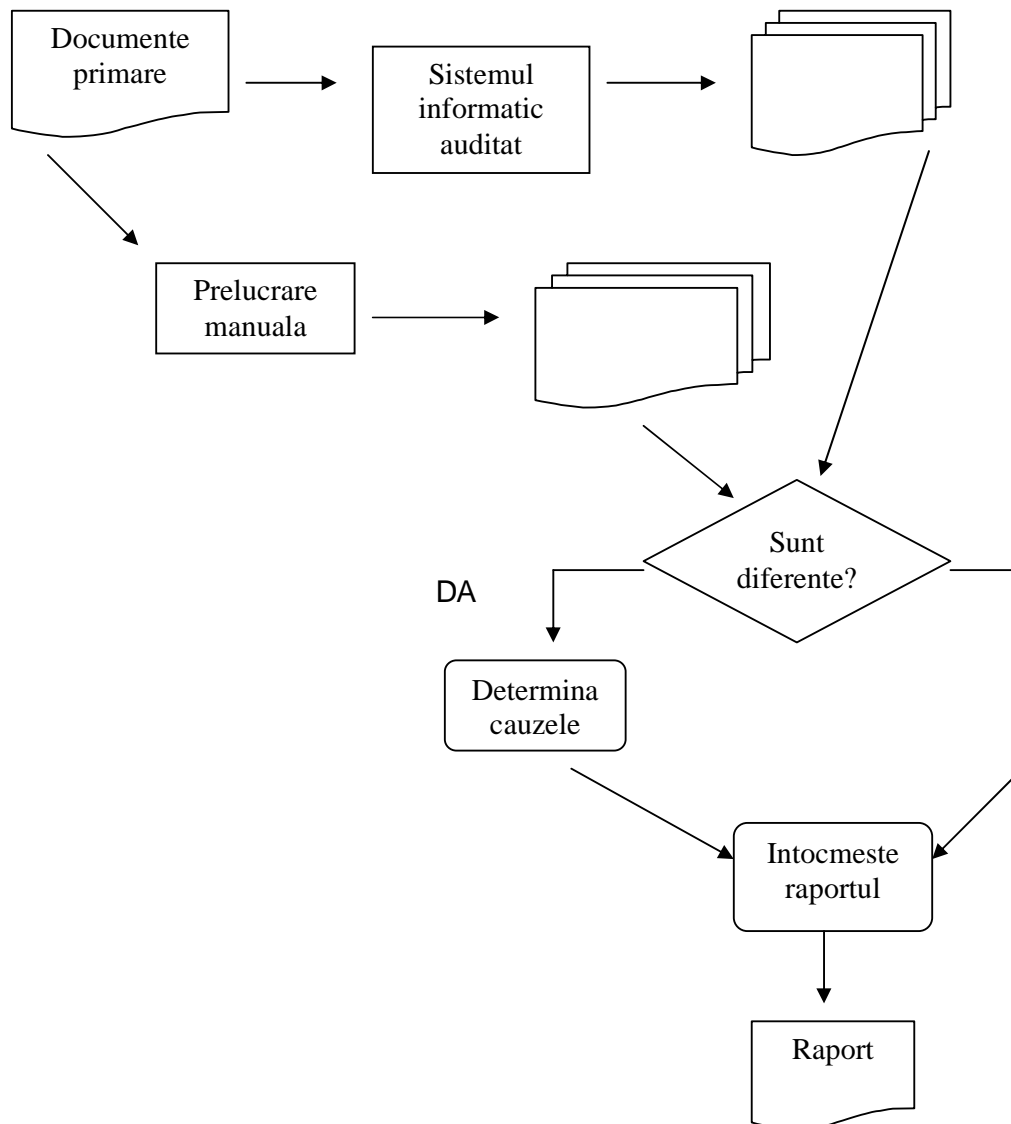
- *Programe utilitare* – programe care nu sunt proiectate pentru scopuri de audit. Realizeaza sortari, creari de fisiere, listari de fisiere, copieri etc.
- Pasii de parcurs in aplicarea unui CAAT:
- Stabilirea obiectivului CAAT;
 - Determinarea continutului si accesibilitatii la fisierele sistemului auditat;
 - Definirea tipurilor de tranzactii ce vor fi testate;
 - Definirea procedurilor aplicate datelor;
 - Definirea cerintelor cu privire la iesiri;
 - Identificarea personalului de audit si operatorilor care pot participa in proiectarea si aplicarea CAAT;
 - Estimarea costurilor si beneficiilor;
 - Asigurarea ca utilizarea CAAT este controlata si documentata corespunzator;
 - Organizarea activitatiilor administrative, asigurarea aptitudinilor necesare personalului implicat si a facilitatilor computerizate;
 - Executarea aplicatiei CAAT;
 - Evaluarea rezultatelor.



Auditarea prin calculator (cu date de test)

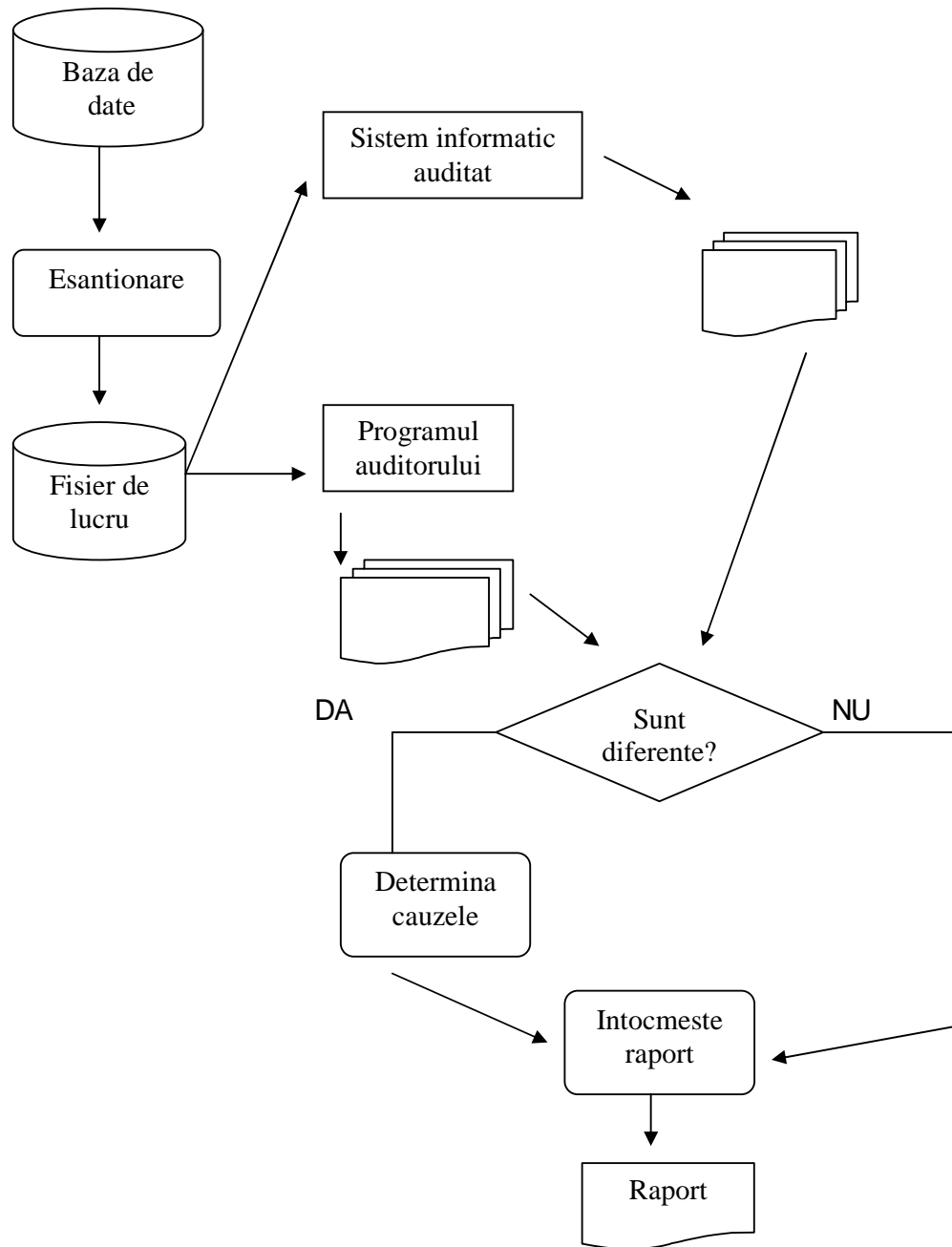
Verificarea autorizarii programelor

- Intrebari:
- Se foloseste doar soft autorizat?
 - Se exploateaza versiunea corecta?
 - Exista soft freeware instalat? Este autorizat de persoanele imputernicite din firma?
- Sunt stabilite persoanele care au dreptul sa faca instalari de noi programe, modificari in programele exploatate si modificari in fisiere? Se respecta aceste restrictii?



Auditarea in afara calcutorului

- Se introduce in cadrul aplicatiei o procedura care sa insereze in prelucrare, la intervale aleatorii, datele de test.
- La sfarsitul testarii fisierele aplicatiei trebuie aduse in starea lor corecta (fara tranzactiile de test inserate de programul auditorului).



Auditarea cu ajutorul calculatorului