

Capitolul 3

CONTROLUL GENERAL AL SI STEMELOR I NFORMATI ONALE

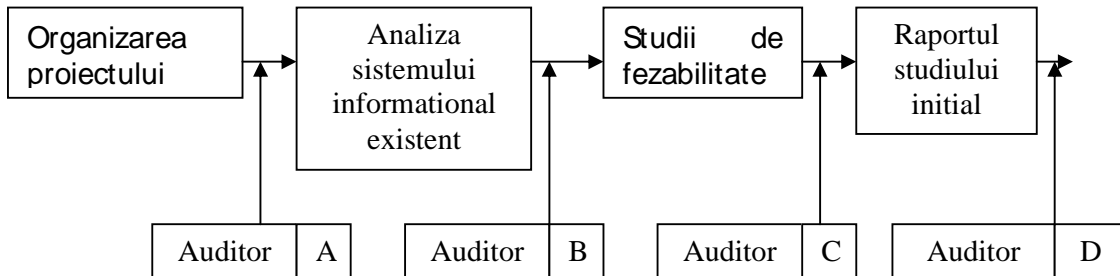
- A. CONTROL LA NIVELUL MANAGEMENTULUI :
- evaluarea anuala a sistemului informational
 - directiile de dezvoltare
 - strategiile de dezvoltare
- B. CONTROLUL CICLULUI DE VIATA
- Controlul initierii proiectului sistemului informational
 - Controlul analizei si proiectarii initiale a sistemului informational
 - Controlul achizitiei (dezvoltarii) sistemului informational
 - Controlul testarii sistemului informational
 - Controlul implementarii si conversiei sistemului informational
 - Controlul intretinerii sistemului informational
- C. CONTROLUL SECURITATII SI STEMULUI
- Responsabilitatea managementului
 - Separarea functiilor incompatibile
 - Controlul accesului
 - Controlul securitatii fizice
 - Controlul prevenirii efectelor dezastrelor
- D. CONTROALELE NIVELULUI OPERATIONAL
- Controlul modului de operare
 - Controlul retelei de calculatoare
 - Controlul pregatirii si introducerii datelor in sistem
 - Controlul procesarii datelor
 - Controlul gestiunii mediilor de stocare
 - Controlul gestiunii aplicatiilor si a documentatiilor
 - Controlul asistentei tehnice
- E. EVALUAREA PERFORMANTELOR SI STEMULUI

CONTROLUL CICLULUI DE VIATA

I. Controlul initierii proiectului

- Realizarea sistemului (achizitia) in corelatie cu dezvoltarea societatii
- Determinarea costurilor, economicitatii sau alte avantaje

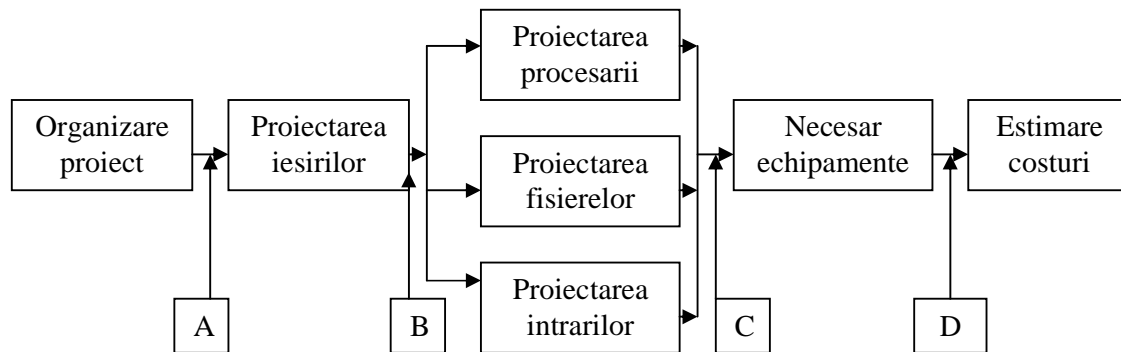
Auditorul – membru al echipei de proiectare



- A. - STRUCTURAREA CORESPUNZATOARE A ECHIPEI DE LUCRU
- B. - REVIZUIREA ANALIZEI SISTEMULUI INFORMATIONAL EXISTENT
- C. - REVIZUIREA COSTURILOR NOULUI SISTEM
- D. - REVIZUIREA DOCUMENTATIEI PROIECTARII CONCEPTUALE

II. Controlul analizei si proiectarii initiale

Scop general - Sistemul dezvoltat (achizitionat) corespunde cerintelor utilizatorului



- A. - REVIZUIREA PROIECTULUI INITIAL
- B. - ASIGURAREA DOCUMENTATIEI
- C. - REVIZUIREA SPECIFICATIILOR FISIERELOR SI INTRARILE ASOCIATE
- D. - REVIZUIREA SPECIFICATIILOR ECHIPAMENTELOR
- E. - REVIZUIREA COSTURILOR SI STANDARDELOR DE PROCESARE

OBIECTIVELE AUDITULUI

Date de intrare {
- tipul
- originea
- volumul si cresterea anticipata
- dependenta temporala

Fisiere {
- tipul {
- principale
- tranzactii
- baze de date
- modul de control si de arhivare
- marimea si cresterea anticipata
- frecventa actualizarii
- relatiile cu fisierele din alte sisteme

Iesiri {
- tipul si continutul rapoartelor
- volumul si cresterile anticipate
- frecventa de raportare
- suportul de prezentare

Altele {
- necesar de hard
- cerintele de securitate
- cerintele legale (soft)
- auditabilitatea (proceduri)

III. Controlul achizitiei (dezvoltarii) sistemului

- Dezvoltarea integrala din interiorul organizatiei (in-house)
- Echipamente achizitionate de organizatie; soft de aplicatie achizitionat de la furnizor (outside)
- Aplicatie integrala la cheie (outsourcing)

- Este necesara proiectarea de detaliu cu interventia specifica a auditorului
- Soft-ul se poate comanda in mod specific
- Criteriile foarte exacte de selectie ale furnizorului

IV. Controlul testarii sistemului

- {
- testare paralela
- testare pilot

Obiectivele auditului :

- {
- asigurarea ca sistemul functioneaza corect
- in cazul intreruperilor, se emit mesaje de documentare
- nu exista prelucrari neefectuate

V. Controlul implementarii sistemului

Obiectivele auditului :

- controlul atribuirii responsabilitatilor la implementare
- controlul standardelor de eficacitate a implementarii
- controlul planului de implementare
- controlul modului de implicare a utilizatorilor la implementare

VI. Controlul intretinerii sistemului

Obiectivele auditului :

- identificarea factorilor care genereaza necesitatea modificarii sistemului
- controlul autorizarii executiei modificarii
- controlul mecanismelor ce previn modificari neautorizate

Factorii care impun modificari ale sistemului :

- Aparitia de functii noi
- Necesitatea modificarii raportarii
- Modificari in cadrul legislativ
- Aparitia de probleme neprevazute in proiectare

CONTROLUL SECURITATII SISTEMELOR INFORMATICE

Procesele de asigurare a securitatii sistemelor informatice indeplinesc functia de a proteja sistemele impotriva folosirii, publicarii sau modificarii neautorizate, distrugerii sau pierderii informatiilor stocate.

Securitatea sistemelor informatice este asigurata prin controale logice de acces, care asigura accesul la sisteme, programe si date numai utilizatorilor autorizati.

Elemente de control logic care asigura securitatea sistemelor informatice :

- cerintele de confidentialitate a datelor;
- controlul autorizarii, autentificarii si accesului;
- identificarea utilizatorului si profilele de autorizare;
- stabilirea informatiilor necesare pentru fiecare profil de utilizator;
- controlul cheilor de criptare;
- gestionarea incidentelor, raportarea si masurile ulterioare;
- protectia impotriva atacurilor virusilor si prevenirea acestora;
- firewalls;
- administrarea centralizata a securitatii sistemelor;
- training-ul utilizatorilor;
- metode de monitorizare a respectarii procedurilor IT, teste de intruziune si raportari.

Obiective de control detaliate

Asigurarea securitatii sistemelor informatice

1. Controlul masurilor de securitate

Securitatea sistemelor informatice trebuie organizata astfel incat sa fie in concordanta cu obiectivele de afaceri ale organizatiei:

- includerea informatiilor legate de evaluarea riscurilor la nivel organizational in proiectarea securitatii informatice;
- implementarea si actualizarea planului de securitate IT pentru a reflecta modificarile intervenite in structura organizatiei;
- evaluarea impactului modificarilor planurilor de securitate IT, si monitorizarea implementarii procedurilor de securitate;
- alinierea procedurilor de securitate IT la procedurile generale ale organizatiei.

2. Identificarea, autentificarea si accesul

Accesul logic la resursele informatice trebuie restrictionat prin implementarea unor mecanisme adecvate de identificare, autentificare si acces, prin crearea unei legaturi intre utilizatori si resurse, bazata pe drepturi de acces.

3. Securitatea accesului on-line la date

Intr-un mediu IT on-line trebuie implementate proceduri in concordanta cu politica de securitate, care presupune controlul securitatii accesului bazat pe necesitatile individuale de accesare, adaugare, modificare sau stergere a informatiilor.

4. Managementul conturilor utilizator

Conducerea organizatiei trebuie sa stabileasca proceduri care sa permita actiuni rapide privind crearea, atribuirea, suspendarea si anulara conturilor utilizator. O procedura formala in raport cu gestionarea conturilor utilizator trebuie inclusa in planul de securitate.

5. Verificarea conturilor utilizator de catre conducere

Conducerea trebuie sa dispuna de o procedura de control care sa verifice si sa confirme periodic drepturile de acces.

6. Verificarea conturilor utilizator de catre utilizatori

Utilizatorii trebuie sa efectueze periodic controale asupra propriilor lor conturi, in vederea detectarii activitatilor neobisnuite.

7. Supravegherea securitatii sistemului

Administratorii sistemului informatic trebuie sa se asigure ca toate activitatile legate de securitatea sistemului sunt inregistrate intr-un jurnal, si orice indiciu referitor la o potentiala violare a securitatii trebuie raportata imediat persoanelor responsabile.

8. Clasificarea datelor

Conducerea trebuie sa se asigure ca toate datele sunt clasificate din punct de vedere al gradului de confidentialitate, printr-o decizie formala a detinatorului datelor. Chiar si datele care nu necesita protectie trebuie clasificate in aceasta categorie printr-o decizie formala. Datele trebuie sa poata fi reclasificate in conditiile modificarii ulterioare a gradului de confidentialitate.

9. Centralizarea identificarii utilizatorilor si drepturilor de acces

Identificarea si controlul asupra drepturilor de acces trebuie efectuate centralizate pentru a asigura consistenta si eficienta controlului global al accesului.

10. Rapoarte privind violarea securitatii sistemului

Administratorii de sistem trebuie sa se asigure ca activitatile care pot afecta securitatea sistemului sunt inregistrate, raportate si analizate cu regularitate, iar incidentele care presupun acces neautorizat la date sunt rezolvate operativ. Accesul logic la informatii trebuie acordat pe baza necesitatilor stricte ale utilizatorului (acesta trebuie sa aiba acces numai la informatiile care ii sunt necesare).

11. Gestionarea incidentelor

Conducerea trebuie sa implementeze proceduri de gestionare a incidentelor legate de securitatea sistemului, astfel incat raspunsul la aceste incidente sa fie eficient, rapid si adecvat.

12. Increderea in terte parti

Organizatia trebuie sa asigure implementarea unor proceduri de control si autentificare a tertilor cu care intra in contact prin medii electronice de comunicare.

13. Autorizarea tranzactiilor

Politica organizatiei trebuie sa asigure implementarea unor controale care sa verifice autenticitatea tranzactiilor precum si identitatea utilizatorului care initiaza tranzactia.

14. Prevenirea refuzului de acceptare a tranzactiei

Sistemul trebuie sa permita ca tranzactiile efectuate sa nu poata fi negate ulterior de nici un participant. Aceasta presupune implementarea unui sistem de confirmare a efectuarii tranzactiei.

15. Informatiile sensibile trebuie transmise numai pe un canal de comunicatii considerat sigur de parti, care sa nu permita interceptarea datelor

16. Protectia functiilor de securitate

Toate functiile organizatiei legate de asigurarea securitatii trebuie protejate in mod special, in vederea mentinerii integritatii acestora. Organizatiile trebuie sa pastreze secrete procedurile de securitate.

17. Managementul cheilor de criptare

Conducerea trebuie sa defineasca si sa implementeze proceduri si protocoale pentru generarea, modificarea, anularea, distrugerea, certificarea, utilizarea cheilor de criptare pentru a asigura protectia impotriva accesului neautorizat.

18. Prevenirea, detectarea si corectarea programelor distructive

In vederea protejarii sistemului impotriva aplicatiilor distructive (virusi), trebuie implementata o procedura adecvata care sa includa masuri de prevenire, detectare, actiune, corectare si raportare a incidentelor de acest fel.

19. Arhitecturi Firewall si conectarea la retele publice

In cazul in care sistemul organizatiei este conectat la Internet sau alte retele publice, programe de protectie adecvate (firewalls) trebuie implementate pentru a proteja accesul neautorizat la resursele interne ale sistemului.

20. Protectia valorilor electronice

Conducerea trebuie sa asigure protectia si integritatea cardurilor si a altor dispozitive folosite pentru autentificare sau inregistrare de date considerate sensibile (financiare).

SECURITATEA SI STEMELE INFORMATI ONALE

RESPONSABILITATI

Organizatia trebuie sa aiba o politica se securitate informationala.

- Responsabilitatile personalului
- Atributiile responsabilului cu securitatea
- Clarificarea datelor si nivelurile de securitate
- Controlul (auditul) intern al securitatii

Politica de securitate se refera la tot personalul angajat :

- standarde interne si principii privind securitatea S.I.

- la nivel global
- pe grupe (functii, sectii) de lucru

- codul etic al angajatilor si pregatirea acestora.

SEPARAREA FUNCTIILOR INCOMPATIBILE

- Limiteaza erorile si fraudele
 - Creste probabilitatea detectarii fraudelor
- Separarea functiilor se realizeaza in domeniile :

- initierea si autorizarea tranzactiilor
- inregistrarea tranzactiilor
- custodia activelor

Persoane diferite pentru operatiile :

- programare – operare
- procesare date – pregatire
- gestionar memorie externa – operator
- eliberare, multiplicare, distrugere informatii – autorizare
- programare – administrare baza de date
- responsabil securitate – orice alte activitati
- controlul drepturilor de acces – alte functii (activitati)

AUTORIZAREA UTILIZATORILOR

1. Identificare : calculatorul recunoaste un potential utilizator al sistemului
2. Autentificare : functia de stabilire a validitatii identitatii pretinse
3. Autorizare : utilizatorului recunoscut i se permite accesul la resursele sistemului

CONTROLUL ACCESULUI

Riscurile accesului neautorizat :

- Diminuarea confidentialitatii
- Furtul informatiilor
- Divulgarea neautorizata de informatii
- Diminuarea integritatii informatiilor
- Intreruperea functionarii sistemului

Controlul accesului in mediile publice utilizand FIREWALL

Impune o politica de control a accesului intre doua retele.

- Intreg traficul de date trece prin el
- Este permisa numai trecerea autorizata prin politica locala de securitate
- Sistemul insusi este imun la penetrare

- Monitorizarea comunicatiilor TCP/IP
- Poate inregistra toate comunicatiile
- Poate fi folosit la criptare.

ETAPELE ATACULUI LA O RETEA

I. Colectare de informatii

- Protocol SNMP - examineaza tabela de rutare pentru un router neprotejat
- Programe TRACE ROUTE - ofera adresele retelelor si routelor intermediare spre o tinta
- Serverele DNS - pot fi interogate pentru a obtine informatii referitoare la tipul calculatoarelor, numele si adresele IP asociate
- Protocol FINGER - informatii despre utilizatorii unui calculator gazda – login, nr. telefon, data ultimei conectari
- Programul PING - determina daca un calculator e disponibil

II. Testarea securitatii sistemelor

- Program de scanare a securitatii sistemelor
 - ISS (INTERNET SECURITY SCANNER)
 - SATAN (SECURITY ADMINISTRATOR TOOL FOR AUDITING NETWORK)
- Programe proprii pentru conectare la porturile specifice ale serviciilor vulnerabile.

III. Accesarea sistemelor protejate

- obtinerea accesului (privilegiat)
- instaleaza SNIFEER – program de monitorizare a pachetelor din retea pentru a obtine nume de conturi si parole.

Avantajele folosirii FIREWALL

- Concentrarea securitatii la server sau nod de retea
- Impunerea unei politici de acces la retea
- Asigura protectia serviciilor vulnerabile NFS, MIS, FINGER
- Monitorizeaza si furnizeaza statistici cu privire la folosirea retelei

Limitele unui FIREWALL

- Restrictioneaza, blocheaza accesul la unele servicii TELENET, FTP
- Protectie scazuta pentru atacuri din interior
- Protectie scazuta fata de virusi
- Diminueaza viteza de comunicare cu exteriorul
- Fiabilitate redusa datorita centralizarii.

Componente FIREWALL

A. ROUTER cu filtrare de pachete

Regulile de filtrare sunt impuse de administratorul sistemului.

Criterii de organizare a filtrului :

- Adresa IP a sursei
- Adresa IP a destinatiei
- Portul sursa TCP/UDP
- Portul destinatie TCP/UDP

B. *SERVERELE PROXY* = se interpun intre client si serverul REAL si permite transferul de date conform politicii de securitate. Monitorizeaza toate comunicatiile.

Realizeaza controlul la nivelul aplicatiei :

- autentificarea utilizatorilor interni si externi
- filtrarea individuala a operatiilor protocolului
- monitorizare

C. *Poarta la nivel de circuit* – este un proxy local.

Functioneaza ca un filtru de pachet.

ARHITECTURI FIREWALL

I. FIREWALL TIP FILTRU DE PACHETE

Principii = tot ce nu este permis explicit este interzis.

II. FIREWALL TIP CALCULATOR GAZDA PROTEJAT

Este format din = router de filtrare
 = statie bastion (proxy)

III. FIREWALL TIP SUBRETEA PROTEJATA

- doua routere de filtrare
- statie bastion (proxy)

OFERTE DE FIREWALL :

- NETWALL <http://www.bull.com>
- PIX FIREWALL www.cisco.com
- EAGLE www.raptor.com
- SUNSCREEM www.incog.com

CONTROLUL SECURITATII FIZICE

- **Auditorul verifica masura in care accesul fizic la date si resursele hardware sunt restrictionate corespunzator :**

- Cum este restrictionat accesul fizic la facilitatile IT din firma?
- Cum este restrictionat accesul la spatiile unde se afla echipamentele pe care se realizeaza prelucrarile?
- Cum sunt protejate stocarile offline de date?
- Cat de sigura, din punct de vedere informational, este scoaterea din uz a calculatoarelor si mediilor de stocare a datelor?
 - Existenta unor programe gen Easy Recovery sau Lost & found care permit recuperarea datelor sterse de pe mediile de stocare. Comanda UNFORMAT din DOS.

⇒ dificultatea asigurarii controlului accesului fizic la fiecare componenta hardware

⇒ extinderea lucrului in retea si a utilizarii sistemelor distribuite s-a caracterizat prin concentrarea atentiei pe controlul accesului logic, dar controlul accesului fizic ramane in continuare important, el reprezentand o componenta a sistemului de securitate.

COPII DE SIGURANTA SI EVENIMENTE NEPREVAZUTE

- **Auditorul trebuie sa verifice daca la nivelul organizatiei exista :**

- Proceduri prin care sa se asigure functionarea sistemului in cazul caderii alimentarii cu energie electrica sau a cailor de comunicatii.
 - Exista sectoare "sensibile" – bancar, bursier, securitatea statului, energetic etc. care impun asigurarea functionarii continue a sistemelor informatice ceea ce implica existenta unor surse alternative de energie si/sau comunicatii.
- Planuri bine testate si documentate, actualizate periodic prin care sa se asigure operationalitatea sistemului informatic in conditiile producerii unor evenimente neprevazute.
- Proceduri si controlul aplicarii acestora, privind realizarea copiilor de siguranta si refacerea starii sistemului in cazul "caderii" acestuia ca urmare a unor cauze hard sau soft.
- Existenta unui contract de asigurare a organizatiei pentru evenimente neprevazute.
- Nivelul de instruire a personalului cu privire la procedurile aplicabile in cazul realizarii periodice a copiilor de siguranta sau executarii procedurilor de criza in cazul producerii dezastrelor.

- **Dezastre :**

- actiuni cu scop distructiv produse intentionat sau nu, inclusiv VIRUSI
- dezastre naturale

Conceptul de BUSINESS CONTINUITY MANAGEMENT (BCM) :

→ anticiparea incidentelor care pot afecta functiile critice si procesele organizatiei asigurand ca organizatia va raspunde oricarui incident conform planurilor elaborate pana la revenirea activitatii la o desfasurare normala.

→ functia IT este una din functiile critice ale organizatiei.

→ plan de actiune care cuprinde proceduri si persoanele responsabile cu punerea in practica a actiunilor de limitare a distrugerilor si refacerea sistemului :

- Stabilirea echipei responsabile cu realizarea unui plan de refacere a sistemului formata din personalul din compartimentul de specialitate, auditorul sistemului informatic, utilizatori.
- Elaborarea procedurilor de verificare a principalelor componente ale sistemului (date, soft, hard, documentatii) in cazul producerii evenimentelor distructive si stabilirea responsabilitatilor.
- Stabilirea locatiilor in care vor fi pastrate copiile de siguranta, documentatiile si componente hardware.
- Stabilirea prioritatilor privind procedurile ce trebuie efectuate.
- Stabilirea locatiei in care se vor executa procedurile.
- Testarea planului pe elemente componente.
- Documentarea planului

→ Nu toate incidentele (evenimentele distructive) pot fi anticipate prin BCM

→ Planificarea continuitatii activitatii in cadrul organizatiei implica aspectele functiei IT :

- Ce a facut managementul privitor la riscul de “cadere” a sistemului si fata de scenariul de dezastre.
- Cum sunt testate si actualizate planurile de continuitate a activitatii :
 - Revederea planurilor existente
 - Sunt clar precizate responsabilitatile?
 - Care este nivelul de instruire a personalului implicat?

NOTA : “Riscul” anului 2000 a reprezentat un eveniment pentru care BCM a trebuit sa prevada un plan de actiune.

- **Refacerea in cazul esecului operational**

Auditorul verifica :

- daca sunt stabilite proceduri adecvate in cazul producerii unor esecuri operationale
- daca aceste proceduri sunt verificate si aprobate de staff-ul IT
- daca aceste esecuri operationale sunt identificate, rezolvate la timp, comsemnate si raportate
- in ce masura echipamentele sunt adecvat plasate si protejate pentru a se preveni riscul distrugerii accidentale (foc, fum, praf, vibratii, radiatii electromagnetice etc.)
- in ce masura echipamentele sunt corect intretinute
- ce controale exista pentru prevenirea esecurilor operationale produse din :
 - cauze hardware
 - neaplicarea corecta a procedurilor de operare
 - erori software
- care sunt procedurile de RESTART si REFACERE (Recovery) pentru refacerea starii sistemului in urma unui esec operational
- in caz de incidente sunt evaluate actiunile operatorilor pentru a se vedea daca prin actiunile lor nu au afectat calitatea prelucrurilor sau structurile de date.

- **BACKUP**

Actualizarile folosind backup-urile datelor (fisierelor), aplicatiilor si software-ul de sistem trebuie sa fie posibile in caz de urgenta :

- Sunt procedurile de backup (pentru date si soft) cele potrivite?
- Sunt backup-urile corect jurnalizate si stocate in locatii sigure?

- Exista siguranta ca backup-urile si procedurile RECOVERY vor lucra la nevoie?

- Datele din fisierele copii sunt acoperitoare pentru refacerea fisierelor operationale?

- Frecventa realizarii copiilor este direct proportionala cu volumul tranzactiilor si importanta datelor pentru organizatie
- Conform procedurilor backup copiile pot fi :
 - partiale
 - totale
- Cea mai populara tehnica de backup este GFS (bunic-tata-fiu) :
 - se fac copii zilnice
 - copia zilnica se va rescrie in saptamana urmatoare
 - la sfarsitul saptamanii se realizeaza "copia saptamanii" (corespunde ultimei copii zilnice)
 - copia saptamanii se reface in luna urmatoare
 - la sfarsitul fiecărei luni se realizeaza "copia lunii". Aceasta se reface in trimestrul sau anul urmator

- **SOFTWARE BACKUP**

- Copii ale sistemului de operare si ale aplicatiilor (se realizeaza in masura in care licenta permite acest lucru)
- Copiile trebuie pastrate in loc sigur (chiar alte locatii decat sediul firmei).

- **HARDWARE BACKUP**

- Achizitionarea unui al doilea sistem care poate fi :
 - Un sistem STANDBY HOT : poate prelua imediat functia sistemului operational
 - Un sistem STANDBY COLD : stocat separat si la nevoie conectat pentru a putea fi folosit
- Incheierea unui contract cu o firma al carei sistem de procesare a datelor are aceleasi facilitati si poate sa suporte prelucrările firmei al carui sistem nu mai este operational
- Apelarea la o firma care ofera servicii in acest domeniu
- Contractele de service cu furnizorul hardware sa prevada furnizarea, pe timp limitat, a echipamentelor care vor inlocui pe cele avariate.
- SISTEME DUPLICATE :
 - specifice domeniilor cu risc mare : banci, burse, etc.
 - au locatii geografice separate pentru minimalizarea riscului de mediu
 - actualizarea simultana, prin tranzactiile curente atat a sistemului operational cat si pe cel duplicat.

CONTROLUL NIVELULUI OPERATIONAL

Distribuirea prelucrării → impune controlul la nivel operational

Activități auditate :

1. Operarea eficientă la postul de lucru

- restricționarea accesului
- utilizarea eficientă a timpului de lucru
- întreținerea și repararea echipamentului
- cunoașterea și respectarea procedurilor de către utilizatori

2. Rețeaua de calculatoare

- Modul de monitorizare a traficului pe rețea
- Politica antivirus – server sau post de lucru
- Controlul politicilor de acces și restricționare
- Protecția conexiunii la rețele publice

Auditorul urmărește :

- Controlul rețelei/accesului dial-up:
- Accesul de la distanță la SI (prin conexiunile la rețea sau dial-up) trebuie să fie restricționate corespunzător:
 - Cum sunt autentificate conexiunile de la distanță la calculatoarele organizației?
 - Dacă rețeaua este mare, în ce măsură este organizată pe domenii separate?
 - Dacă rețeaua este partajată (mai ales dacă se extinde dincolo de organizație) ce controale există pentru a se verifica faptul că utilizatorii accesează doar porțiunile de rețea pentru care sunt autorizați?
 - Cum sunt protejate transmisiile în rețea?
 - Dacă este corespunzător numărul de utilizatori dial-up?
 - Cum sunt autentificați utilizatorii dial-up?
 - În ce măsură disponibilitatea facilităților dial-up este restricționată la momentele de timp (zi/săptămână)?
 - Ce controale se folosesc pentru diagnosticul porturilor?
- Controlul conexiunilor externe la rețea (Internet, EDI, EFT)
 - Conexiunile externe trebuie folosite doar pentru scopuri valide ale afacerii și controalele trebuie să prevină ca aceste conexiuni să submineze securitatea sistemului
 - În ce măsură aceste conexiuni externe sunt impuse de nevoile organizației?
 - Cât de sigură este poșta electronică a organizației?
 - Cât de bine este protejat gateway-ul dintre Internet și mediul firmei?
 - Ce controale există pentru a preveni accesarea unor site-uri inadecvate?
 - Ce controale există pentru a preveni navigarea neproductivă pe Internet a personalului și în afara sarcinilor de serviciu?
 - Cât de bine sunt protejate conexiunile externe ale rețelei pentru folosirea EDI și EFT?
 - Soluția hardware și software a rețelei trebuie să asigure nevoile de disponibilitate, performanță și flexibilitate.
 - Ce documentație de rețea este disponibilă?

- Cum sunt aprobate modificarile din retea, controlate si testate?
- Ce procese au loc pentru planificarea capacitatii si monitorizarea nivelului de performanta?

3. Pregatirea datelor si introducerea in sistem

- Pregatirea documentelor primare
 - Datele sunt clasificate, grupate, verificate, sortate si transmise pentru procesare.
- Controlul introducerii datelor
 - Acuratetea datelor depinde de :
 - calitatea controalelor
 - factorul uman
 - tipul echipamentelor folosite pentru introducerea datelor in sistem.

4. Procesarea datelor

- Acces autorizat pentru declansarea procedurilor
- Respectarea termenelor si timpilor de procesare
- Protejarea fisierelor
- Pastrarea rezultatelor procesarii

Auditorul va verifica cum managementul controleaza masura in care rolul si responsabilitatile personalului implicat in procesarea datelor sunt cunoscute si respectate, focalizand pe procedurile de :

- backup si refacerea sistemului
- preluarea pe loturi (batch) si/sau on-line. Asigurarea la timp a datelor necesare prelucrarilor, mai ales in cazul in care acestea sunt asigurate de alte sisteme informatice (interne sau externe organizatiei)
- intretinerea software-ului.

Auditorul va urmari masura in care a asigurat documentatia necesara personalului implicat in procesarea datelor.

5. Gestionarea mediilor de stocare

Pastrarea, utilizarea si intretinerea :

- dischetelor
- CD-urilor
- HDD-urilor
- casetelor cu banda (data cartdrige)
- casetelor zip

Jurnalul de evidenta a mediilor de stocare cuprinde :

- identificatorul (eticheta) mediului de stocare
- localizarea curenta

- persoana responsabila (gestionarul)
 - data achizitiei
 - utilizatorul
 - fisierele/programele/aplicatiile continute
 - persoanele autorizate sa acceseze mediul
 - data ultima cand a fost folosit? De cine? Data restituirii?
 - data la care continutul poate fi sters
- Cum sunt protejate stocarile offline de date?

6. Gestionarea aplicatiilor si a documentatiei

- modul de pastrare
- modul de acces
- actualizarea documentatiei
- copii de siguranta.

7. Asistenta tehnica

- modul de achizitionare a hardware-ului
- instruire utilizatori
- identificarea erorilor de procesare si modul de rezolvare
- controlul soft-urilor
- raportarea incidentelor.

Managementul trebuie sa stabileasca nivelurile de service necesitate de utilizatori si sa stabileasca politicile privind asigurarea acestora :

- In ce masura corespund contractele de service existente nevoilor reale?
- In ce masura service-ul asigurat raspunde cerintelor de securitate?

8. Monitorizarea performantelor

- Monitorizarea performantei operationale si aprobarea procedurilor documentate.

Managementul trebuie sa monitorizeze performanta privitoare la nivelele de service si a procedurilor de operare.

- Ce informatii primeste managerul pentru a-i permite sa monitorizeze starea mediului hard si terminarea la timp a prelucrarilor batch?

- Cat de des se primesc aceste informatii?

- In ce masura au existat probleme cu performanta componentelor hardware si/sau executarea la timp a prelucrarilor batch?

- Ce monitorizare se desfasoara pentru verificarea operarii eficiente a calculatorului?

- In ce masura au existat probleme cu neaprobarea unor proceduri definite pentru operarea calculatorului?