

Capitolul 2

RI SCURI LE ASOCI ATE SI STEMELOR I NFORMATICE

Managementul riscurilor – procesul prin care se identifica si se cuantifica evenimentele ce pot genera pierderi unei organizatii.

Riscurile asociate auditului financiar – Riscul de audit

- a) – Riscul inherent general
 - riscul de management
 - riscul contabil
 - riscul de afaceri
- b) – Riscul de control
 - o eroare sau un grup de erori cu impact semnificativ nu a fost prevenita, detectata sau corectata la timp de sistemul contabil sau auditul intern
- c) – Riscul de nedectare
 - procedurile fundamentale de audit nu detecteaza o eroare semnificativa sau mai multe erori insumate cu efect cumulat semnificativ
- d) – Riscul de esantionare

Auditorul financiar trebuie sa ia in considerare modul in care un mediu CIS afecteaza auditul.

Riscul inherent si riscul de control intr-un mediu CIS poate avea particularitati :

- Riscuri generate de deficiente ale mediului CIS
- Cresterea potentialului de aparitie a erorilor si a activitatilor frauduloase specifice
- O eroare individuala in mediul CIS poate afecta intregul ansamblu informational al intreprinderii

Sursa – STANDARDE DE AUDIT FINANCIAR

RI SCURI LE ASOCI ATE SI STEMULUI I NFORMATI ONAL

- a) Riscurile de mediu
- hardware si retele de comunicatii
 - sistem de operare
 - softuri de aplicatie
 - informatiile procesate de sistem

- b) Riscuri asociate mediului :
- pericole naturale si dezastre
 - alterarea sau furtul aplicatiilor, datelor
 - erori umane sau tehnice
 - incompetenta manageriala
 - pierderi financiare previzibile

- Riscurile trebuie :
- evaluate din punct de vedere al gravitatii efectelor lor
 - evaluate din punct de vedere al probabilitatii procedurilor
 - estimate financiar pentru fiecare aparitie a fenomenului si pe total

Particularitati ale sistemelor informatice in evaluarea riscului :

- A. Structura organizationala
- Concentrarea functiilor si a cunostintelor
 - Concentrarea programelor si a datelor

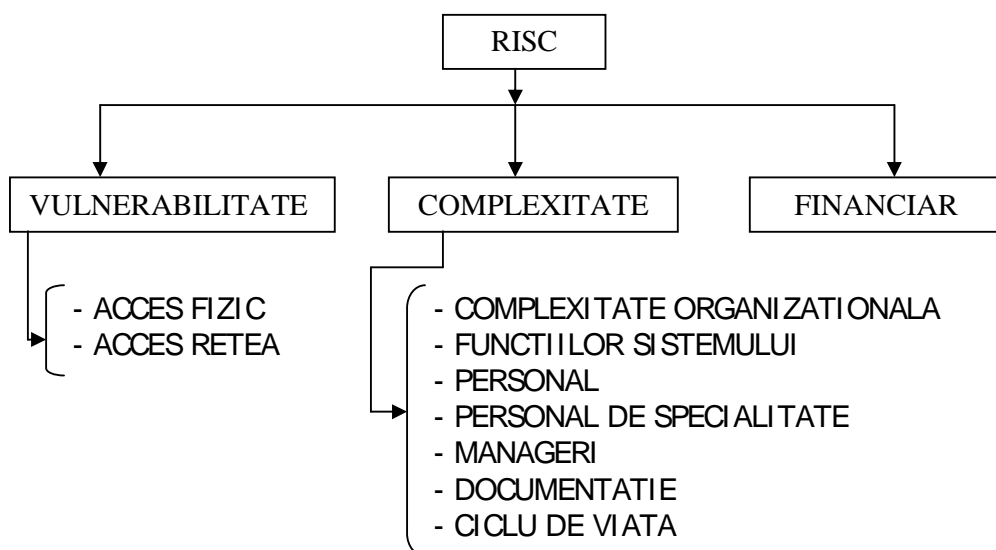
- B. Natura procesarii
- Absenta documentelor de intrare
 - Lipsa unei dovezi vizibile a tranzactiei
 - Lipsa unor iesiri vizibile
 - Usurinta de a accesa datele si softurile

- C. Aspecte procedurale
- consecventa executiei
 - proceduri de control programate
 - o tranzactie are efect in fisiere multiple
 - vulnerabilitatea mediilor de stocare

Riscuri asociate unui sistem informatic :

- a) pierderea, deturnarea, modificarea informatiilor
- b) accesul neautorizat la informatii
- c) intreruperea procesarii

MODEL CALITATIV DE EVALUARE A RISCURILOR



RISCU ASOCIAT ACCESULUI FIZIC

NI VEL RI SC	DESCRI ERE
MARE	Resursele informaționale sunt accesibile tuturor angajaților
MEDIU	Resursele informaționale sunt în birouri organizate cu acces limitat de personal
SCAZUT	Resursele informaționale sunt în zona cu acces strict controlat

RISCU ASOCIAT REȚELEI DE COMUNICATII

NI VEL RI SC	DESCRI ERE
MARE	Sistem conectat la rețeaua publică
MEDIU	Sistem conectat la rețea privată. Comunicarea cu exteriorul cu linii dedicate
SCAZUT	Nici o conexiune cu mediul

Sursa : <http://www.itandit.org/memberana/form/newitanditor/F213.na.htm>

RISURI SI ACCIDENTE DECLANSATE

1. Eroare de operare - Acest risc generează 70-80 % din accidente
 Cazuri = 1980 – declanșarea alertei nucleare în SUA 1992 – suspendarea activității centralei nucleare în Pennsylvania.

2. Functionarea defectuoasa a hardware-ului

Cazuri = 1994 – functionarea defectuoasa a microprocesorului PENTIUM. Pierderea a 475 milioane USD.
1994 (1 august) – NASDAQ nu a functionat 34 minute din cauza defectarii liniilor de comunicatie.
1993 – 24 de cazuri de afectare a zborurilor aviatiei civile prin interferarea cu mijloacele electronice de la bord ale pasagerilor.

3. Functionarea defectuoasa a software-ului

Cazuri = problema anului 2000
1999 – transferuri gresite de sume – BANK OF NW
5 milioane USD.

4. Date eronate nedectate de sistem

Cazuri = Controlul automat imposibil pentru situatia :
Varsta variaza intre 18 si 70 ani
Data reala 10/02/45
Data eronata 10/02/54
1993 – indicele Down Jons a cazut cu 12 puncte din interpretarea gresita a unei comenzi de vanzare :
11 milioane USD → 11 milioane actiuni.

5. Riscuri asociate componentelor nonelectronice

Cazuri = 1991 – operatorul AT&T nu a precizat prioritatea comunicatiilor pentru liniile aeriene – 102 minute nu au functionat radarele aeroporturilor din NW.

6. Riscuri asociate performantelor inadecvate ale sistemului

Cazuri = 1987 – bursa din NW a calculat costul actiunilor in 2 ore (nu in timp real) deoarece volumul vanzarilor a fost de 500 de operatii – de 3 ori mai mult decat normal.

7. Riscuri asociate responsabilitatilor legale

Cazuri = Romania. 87% din softuri sunt pirat.

NIVEL DE VULNERABILITATE

Numar utilizatori autorizati	RISCU L ACCESI BILITATII		
	MARE	MEDIU	SCAZUT
Majoritatea utilizatori autorizati	MARE	MARE	MEDIU
50 % utilizatori autorizati	MARE	MEDIU	SCAZUT
Numar limitat de utilizatori autorizati	MEDIU	SCAZUT	SCAZUT

Riscul complexitatii organizationale

MARE -- Erorile din sistem afecteaza intreaga organizatie

MEDIU – Erorile din sistem afecteaza anumite compartimente

SCAZUT – Erorile din sistem afecteaza un compartiment

Riscul functiilor sistemului

MARE – Functii multiple ce se intersecteaza

MEDIU – Functii multiple independente

SCAZUT – Sistemul realizeaza o singura functie

Riscul asociat personalului

MARE – Personalul nu a fost verificat înainte de angajare si nici in prezent

MEDIU – Personalul este verificat imediat dupa angajare

SCAZUT – Personalul este verificat inainte de angajare

Riscul asociat personalului de specialitate

MARE – O singura persoana se ocupa de tot sistemul

MEDIU – Exista 2-3 persoane ce asigura functionarea si intretinerea sistemului

SCAZUT – Exista mai mult de 3 persoane implicate in functionarea sistemului

Riscul asociat managerilor

MARE – Nici o preocupare a managerilor

MEDIU – Manageri preocupati numai de securitatea sistemelor

SCAZUT – Manageri implicati activ si constant in asigurarea securitatii ca urmare a evenimentelor produse in trecut

Riscul asociat ciclului de viata

MARE – Sistem implementat de cel mult un an si durata de viata este de cel putin 20 ani

MEDIU – Sistem cu durata de viata mai mare de 4 ani

SCAZUT – Sistem cu durata de viata intre 1-4 ani

Riscul asociat documentatiei

MARE – Nu exista documentatie

MEDIU – Documentatia exista, dar nu reflecta realitatea din sistem

SCAZUT – Documentatia este actualizata si este disponibila

Exista softuri specializate in evaluarea riscurilor :

RISK – Simularea riscurilor

BUDDY SYSTEM – Analiza securitatii si managementul riscurilor

RISK PAC – Sistem expert pe baza de chestionar.

Surse :

www.palisade.com

www.buddysystem.net/html/product.shtml

<http://computers.software-directory.com>

MODELUL CANTITATIV DE EVALUARE A RISURILOR

A. FACTORII DE RISC

- AMENINTARI (A) – evenimente exterioare sistemului
- VULNERABILITATI (V) – puncte slabe ale sistemului
- IMPACT (I) – consecinte

$$\text{RISC} = A \times V \times I$$

Clasificare calitativa	- RISC MARE	3
	- RISC MEDIU	2
	- RISC REDUS	1
	- RISC INEXISTENT	0

ia

$$\text{RISCU L GENERAL} = \text{valori intre 0 si 27}$$

B. FACTORII DE RISC SI ELEMENTE COLATERALE

- pierderea anticipata anualizata	PAA
- rata aparitiei	RA
- factorul de vulnerabilitate	FV
- pierderea potentiala	PP
- riscul unei singure pierderi	RSP

$$\text{PAA} = \text{RA} \times \text{PP} \times \text{FV}$$

Calculat pentru fiecare pereche activ – amenintare

Tipuri de pierderi :

- Fraude realizate prin intermediul sistemului
- Divulgarea neautorizata de informatii
- Furturi de echipamente
- Distrugerea fizica a echipamentelor

METODE DE MINIMIZARE A RISULUI

IMPERATIVE :

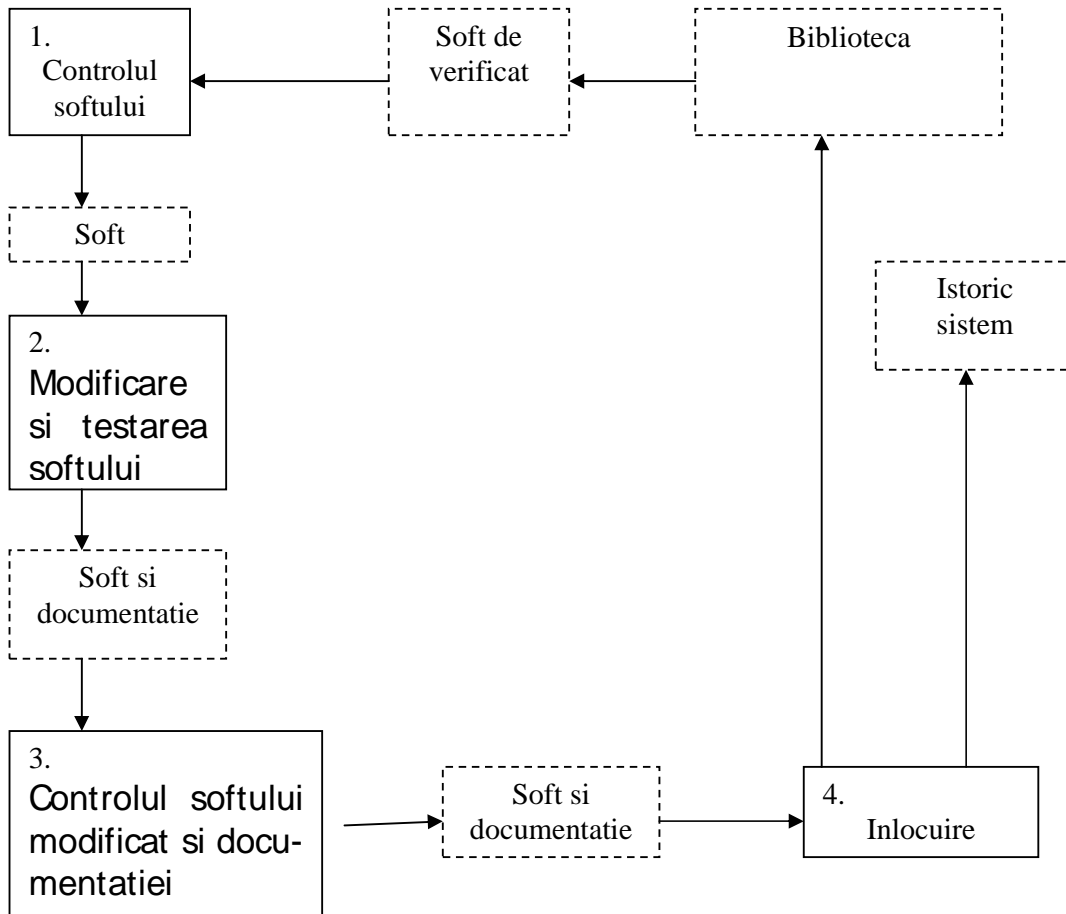
- Creeaza din start un sistem informatic corect
- Pregateste utilizatorii pentru procedurile de securitate
- Odata sistemul pornit, mentine securitatea sa fizica
- Securitatea fizica asigurata, previne accesul neautorizat
- Avand controlul accesului, se asigura ca reluarile de proceduri sa fie corecte
- Chiar daca exista proceduri de control, cauta cai de a-l perfectiona
- Chiar daca sistemul pare sigur, auditeaza-l si identifica noi probleme de securitate

- Chiar daca este foarte vigilent, pregateste-te de dezastre

CAI :

1. Dezvoltarea si modificarea sistemului de control

- Orice modificare de soft trebuie verificata
- Asigurarea documentatiei la zi
- Asigurarea cu softuri specializate antivirus la zi



2. Pregatirea personalului pentru reducerea riscului

- periodicitate
- selectie

3. Mentinerea securitatii fizice

- acces fizic restrans

4. Controlul accesului la date, hardware si retele

- controlul operatiunilor vamale
- definirea exacta a accesului privilegiat
- eliminarea intruziunilor
 - parole
 - carduri ID
 - chei hardware
 - control – retinei, amprentei digitale palmare etc.

- criptare si decriptare date.

Controlul accesului pe baza :

- a ce stii
- a ce ai
- a ce esti
- locului in care te afli.

5. Controlul tranzactiilor

- segregarea indatoririlor
- validarea datelor
- corectarea erorilor
- Backup