Auditul Securității Informației (ASI)

Motto
în God we trust. Everyone else we audit!
B. Baczko*

Доверяй, но проверяй!

Analiza riscului

Agenda

- De ce este importantă analiza riscurilor TI ?
- Avantajele implementării unui sistem de gestiune a riscurilor
- Gestiunea riscului ca proces
- Identificarea și evaluarea riscului
- Măsuri de reacție la riscuri
- Descrierea riscului

Indiferent de activitate, suntem expuşi riscului şi trebuie să fim suficienţi de rapizi în a-l gestiona corespunzător

Importanta

- Analiza riscului și evaluarea conformității legislației rămân a fi prioritățile companiilor
- Tot mai mult, auditul intern se focusează pe riscurile TI și busines
- Tehnologiile rămîn a fi în top, securitatea informației și protecția datelor cu caracter personal fiind cele mai critice domenii

De ce este importantă analiza riscurilor TI ?

- Nivelul de dependență tot mai inalt al organizațiilor de TI și sistemele informatice
- Complexitatea și diversitatea mijloacelor și a soluțiilor TI utilizate de către organizații
- Dispersia teritorială a organizațiilor
- Insuficiența măsurilor de securitate dar și a celor de identificare a tentativelor de acces nesancționat
- Necesitatea corespunderii legislației și a cerințelor normative înaintate de diferite organisme de reglementare
- Sporirea crimelor informatice la nivel mondial

Avantajele implementării unui sistem de gestiune a riscurilor

- Identificarea oportună, analiza și gestiunea riscurilor TI și busines ce pot afecta negativ realizarea strategiei de busines și a obiectivelor organizației
- Focusarea pe ariile / domeniile de risc înalt și alocarea eficientă a resurselor organizației
- Sporirea eficienței și a siguranței tehnologiilor informaționale, a proceselor TI și busines, optimizarea sistemului de control intern
- Sporirea capacității organizației de a reacționa în cazuri de forță majoră, de a asigura continuitatea și de a prognoza activitatea
- Sporirea nivelului de capitalizare și de imagine a companiei

Ce reprezintă riscul?

- **Risc** – probabilitatea realizării unui eveniment, ce poate influența negativ atingerea obiectivelor
- **Riscul în domeniul businesului** – o amenințare sau o acțiune, realizarea căreia poate influența negativ asupra capacității companiei de a-și atinge obiectivele de activitate
- **Riscul** reprezintă o combinaţie dintre probabilitatea unui eveniment şi consecinţele acestuia (impact)
- Toate tipurile de risc trebuie evaluate în scopul determinării nivelului de acceptanță a riscului pentru companie sau al implementării mecanismelor de control suplimentare în scopul minimizării

Principalele categorii de riscuri TI

Gestiunea riscurilor

- **Gestiunea riscurilor** – proces, realizat de către consiliul directorilor, conducere și alți colaboratori special numiți în acest sens, ce vizează întreaga organizație și are ca scop identificarea, analiza și minimizarea evenimentelor, ce pot influența negativ activitatea acesteia
- Gestiunea riscurilor este un proces continuu ce are ca scop implementarea masurilor de minimizare / evitare a riscului și raportarea informației despre riscurile identificate către conducere și toți colaboratorii organizației
- Gestiunea riscului NU presupune înlăturarea completă a acestora:
  - Este imposibilă minizarea riscului până la un minim absolut
  - Este imposibilă identificarea tuturor surselor de risc
  - Minimizarea unor riscuri necesită costuri sporite
  - Acceptarea unor riscuri permite minizarea costurilor
  - Stabilirea unui nivel limită a riscului permite să stabilim nivelul acceptabil, până la care riscul trebuie minimizat, și care este nivelul riscului ce poate fi acceptat

Evaluarea calitativă și cantitativă a riscurilor

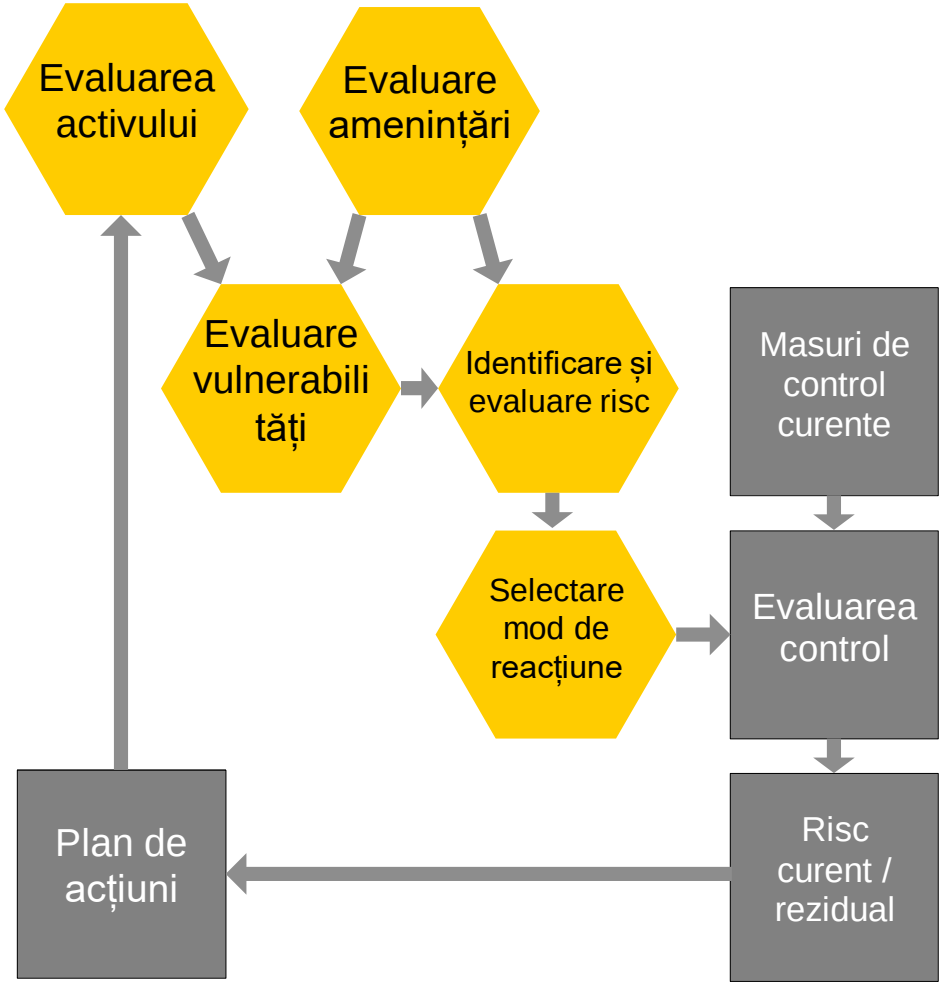
- **Evaluarea cantitativă** – poate fi aplicată atunci când valorile cantitative ce caracterizeaza riscul pot fi calculate (exemplu: rata anuală de realizare, pierderi unice potențiale)
- **Evaluarea calitativa** – se aplică prin impunerea unui sistem evaluare a nivelului de impact (catastrofic, major, moderat, minor, nesemnificativ) și a probabilității de realizare (cert, înaltă, medie, mică, nesemnificativă) a riscului

Totul poate fi prevăzut/calculat ?

- **Loialitatea angajaților și a clienților**
- **Scăderea vânzărilor**
- **Încălcarea obligațiunilor contractuale**
- **Încălcarea obligațiunilor contractuale**
- **Accesibilitatea resurselor financiare**
- **Întârzirerea luării deciziilor**
- **șamd.**

Procesul de gestiune a riscurilor

- **Procesul de gestiune a riscului** – procesul, ce permite 1) balansarea costurilor operaționale și economice pentru implementarea măsurilor de protecție, 2) extinderea funcționalității securizate a sistemelor, 3) sporirea eficienței de gestiune a TI în general, 4) sporirea nivelului de automatizare a proceselor de busines



Sistem de clasificare și evaluare a riscului /redesenat!!!

Probabilitatea:

Nesemnificativ	1
Mica	2
Medie	3
Înaltă	4
Sigur	5

Impact:

Fără semnificație	1
Minor	2
Moderat	3
Major	4
Catastrofic	5

Prioritatea acțiunilor:

Imediat	1
Repede	2
Nu este urgent	3
De a planifica pt viitor	4
Nu sunt necesare	Нет

Risc acceptabil < Risc major		PROBABILITATE				
		Sigur (5)	Înaltă (4)	Medie (3)	Mică (2)	Nesemnificativă(1)
IMPACT	Catastrofic (5)	Critic (25)	Critic (24)	Critic (22)	Major (19)	Minor (15)
	Major (4)	Critic (23)	Critic (21)	Major(18)	Major (14)	Minor (10)
	Moderat(3)	Critic (20)	Major (17)	Major(13)	Major (9)	Minor (6)
	Minor (2)	Major (16)	Major (12)	Major (8)	Minor (5)	Redus (3)
	Fără semnificaţie (1)	Minor (11)	Minor (7)	Minor (4)	Redus (2)	Redus (1)

Evaluarea riscului rezidual:

Controalele existente acoperă riscul complet	0
Controalele existente acoperă riscul însă există probabilitatea, că ele pot funcționa ineficient	1
Controalele existente nu acoperă riscul	2
Controalele existente sunt insuficiente pentru a acoperi riscul	3
Lipsesc controale	4

Model de reacție la risc în funcție de rezultatul evaluării «5Ts & 5Cs»

1. **Terminate** (excludere): se utilizează atunci când nivelul riscului este înalt, este imposibilă aplicarea măsurilor de minimizare a acestuia sau costurile sunt foarte ridicate
2. **Control**: una dintre măsurile cele mai eficiente este sporirea măsurilor de control
3. **Transfer**: Se utilizează atunci când impactul riscului este evaluat a fi înalt iar probabilitatea de realizare joasă. Se aplică transferul în totalitate sau parțial către o terță parte
4. **Contingencies** (rezervarea): o măsură de reacțiune la riscurile cu un impact înalt și cu o probabilitate de realizare joasă. Presupune implementarea mecanismelor / tehnologiilor de rezervare
5. **Take more** (creșterea): în cazul, când impactul și probabilitatea riscului sunt joase, este oportun de căuta soluții de optimizare a resurselor utilizate sau a noilor direcții de investiții
6. **Tolerate** (Acceptare): riscurile cu impact și probabilitate de realizare joase pot fi considerate nesemnificateve și acceptate fară a implementa oarecare măsuri speciale în acest sens
7. **Communicate**: una dintre etapele procesului de gestiune a riscurilor, ce se referă la riscurile cu impact înalt și probabilitate de realizare medie sau minoră. Atunci când controlul nu poate minimiza riscurile respective până la un nivel aceptabil, se recomandă comunicarea despre existența riscului tuturor părților interesate, cu mesajul, că riscul există și potențial poate influența atingerea obiectivelor. Acest aspect adesea este omis
8. **Commission research** (cercetarea): se utilizează atunci când în organizație există un proces matur de gestiune a riscurilor și presupune studiul mai aprofundat al acestora, inclusiv al impactului, probabilității de realizare, efectuarea analizei comparative, etc.
9. **Tell someone** (comunicare terțelor părți): pentru unele riscuri cu un impact sporit și probabilitate de realizare înaltă uneori pot fi propuse măsuri mai eficiente de către companii terțe specializate, decât de către colaboratorii, ce se ocupă de gestiunea riscurilor în organizație
10. **Check compliance** (verificarea conformității): adesea măsura respectivă este ignorată. Abordarea presupune focusarea pe domeniile unde controalele sunt critice din punct de vedere a minimizării riscurilor de conformare legislatiei și presupune verificarea eficienței controalelor

Exemplu: strategii de reacție

Risc	Strategie de reacție
Introducerea în sistemul informatic a informației necorecte în resultatul erorii operatorului	**Acceptarea riscului:** ► Monitorizarea riscului. **Minimizarea riscului:** ► Configurarea sistemului astfel încât erorile operatorului să fie reduse la minim ► Implementarea diferitor controale de detectare a erorilor
Modificarea, pierderea informației sensibile în rezultatul obținerii accesului neautorizat în sistemul informatic	**Minimizarea riscului:** ► Limitarea accesului la sistem doar pentru colaboratorii responsabili, conform necesităților de serviciu ► Implementarea controalelor de monitorizare a accesului în sistemul informatic
Indisponibilitatea echipamentului TI în rezultatul unei situații de forță majoră	**Transferul riscului:** ► Asigurare; ► Contractarea serviciilor unor companii terțe privind prestarea echipamentului conform unor SLA agreate.
Posibilitatea aplicării amenzilor de către organismele regulatorii în cazul transmiterii transfrontalieră a datelor cu caracter personal	**Evitarea riscului:** ► Refuz de a transmite datele cu caracter personal înafara țării.

Descrierea riscului

Riscul trebuie să includă descrierea evenimentului și a urmărilor (sau a beneficiilor ratate) +	Riscul nu trebuie să prezinte lipsa controlului sau a procesului -
Exemplu: ► Insuficiența procedurilor formale în cadrul procesului de gestiune a incidentelor poate duce la implementarea modificărilor incorecte sau neautorizate ► Lipsa persoanelor responsabile de controlul și monitorizarea nivelului de deservire a serviciilor prestate clienților poate duce la prestarea necalitativă a serviciilor și pierderea clienților	Exemplu: ► Modificările din sistem nu sunt autorizate ► Nu au fost numite persoane responsabile de controlul și monitorizarea nivelului de calitate a serviciilor prestate clienților

Exercițiu practic 1. Riscuri TI

Exemplu: evaluarea riscului

- **Descrierea amenințării:** căderi de tensiune electrică
- **Risc**: căderile de tensiune electrice pot duce la pierderi parțiale de date
- **Impactul**: Mediu (3)
- **Probabilitatea realizării**: Înalt (4) – căderile de tensiune au loc regulat, cel puțin de 3 ori săptămânal
- **Nivelul riscului** (corespunzător matricii de riscuri): 17 (Mediu)
- **Mijloace curente de control**:
  - Camerele cu servere sunt dotate cu surse de energie suplimentară cu transfer automat
  - Este realizată monitorizare la distanță 24/24 a modului de funcționare UPS, cu înștiințare automatizată despre incidente
- **Riscul rezidual**: Controalele implementate acoperă riscul, însă există probabilitatea, că acestea nu vor funcționa eficient (1)
- **Prioritatea măsurilor corective**: nu este urgent (3)
- **Măsuri corective**: dublarea liniei de alimentare cu energie electrică pentru a asigura continuitatea curentului electric.

Exemplu: evaluarea riscului

- **Descrierea amenințării:** moartea / dispariția / eliberarea din funcție a specialiștilor TI cheie
- **Risc**: stoparea totală sau temporară procesului de buisines, inaccesibilitatea aplicațiilor/ resurselor TI(mentenanță, activitate operațională), imposibilitatea luării deciziilor
- **Impactul**: Major (4)
- **Probabilitatea realizării**: Medie (3)
- **Nivelul riscului** (corespunzător matricii de riscuri): 18 (Mediu)
- **Mijloace curente de control**:
  - Dublarea funcțiilor anumitor specialiști cheie
  - Pentru unele procese / proceduri /operațiuni critice există elaborată documentație cu descrierea detaliată a activităților (proceduri, instrucțiuni)
- **Riscul rezidual**: controalele curente nu acoperă riscul în totalitate (3)
- **Prioritatea măsurilor corective:** rapid (2)
- **Măsuri corective**: Extinderea masurilor de control menționate pentru toți colaboratorii cheie, procesele și proceduri critice

Exercițiul practic 2. Descrierea și evaluarea riscului