Tehnici de analiza riscului în auditul sistemelor informatice

Lect. Gabriela AVRAM
AISTEDA, Alba Iulia

Auditul sistemelor informaționale *urmărește evaluarea coerenței, calității și securității sistemelor informaționale și informatice, adică a importanței riscurilor aferente informaticii, și testarea cuprinderii și eficacității mijloacelor de control, prevenire și protecție pentru a vedea dacă pot garanta un nivel de risc acceptabil. (conform definiției date de F.I.A.S.I.-La Federation Internationale des Auditeurs et Experts en Systemes d'Information).*

În prezent, se observă o deplasare de la auditul bazat pe viziunea sistemică, spre un audit bazat pe noțiunea de risc. În vreme ce primul considera că orice tranzacție din orice companie poate fi la fel de mult supusă greșelii, cel de-al doilea pretinde auditorului să folosească toate informațiile disponibile pentru a decide dacă erorile nu sunt mai probabile într-un anume domeniu și în raport cu anumite obiective. Această abordare face posibilă direcționarea efortului de audit către acele domenii în care se consideră că riscul de eroare este mai mare.

"Analiza riscului" este o denumire generică pentru un evantai larg de tehnici care permit utilizarea incertitudinii ca factor în cadrul unui plan de acțiune pentru viitor. Articolul de față este consacrat prezentării unei noi tehnici care vine să înlocuiască și să simplifice tehnica chestionarelor de control intern, folosită până în prezent. În plus, ea beneficiază din plin de aportul calculatorului.

Analiza riscului în cadrul acțiunii de audit

În cadrul temporal stabilit pentru audit, auditorii vor trebui îndrumați să-și aloce timpul acolo unde riscul este maxim. Este un adevăr axiomatic că niciodată nu există timp suficient pentru a audita totul în mare adâncime. Auditorii trebuie să fie selectivi. Ei au nevoie de tehnici care să-i sprijine în determinarea domeniilor care pot să beneficieze cel mai mult de pe urma auditului și care să-i ajute să-și împartă timpul între diversele domenii auditate.

Tehnica chestionarului de control intern

În mod tradițional, auditorii se bazau pe chestionarul de control intern (CCI). Chestionarul de control intern este o listă de întrebări asupra controalelor-cheie - răspunsurile respective oferind auditorului informații asupra calității controlului intern. CCI este aplicabil atât în auditurile financiar-contabile, cât și în cele funcționale. Întrebările sunt puse în așa fel încât răspunsurile cu "da" sunt răspunsuri "bune", iar cele cu "nu", răspunsuri "rele". Un chestionar completat oferă o sursă importantă de documentare pentru audit.

Auditorii obișnuiesc să proiecteze chestionare de control intern (CCI) standard pentru domeniile pe care le auditează frecvent. În acest fel, au la îndemână instrumente extrem de folositoare. Ele sunt proiectate de experți în audit, ce se sprijină pe sesiuni de brainstorming și consultări cu manageri bine informați. Chestionarele pot fi modificate din când în când, atunci când experiența dovedește că ele nu acoperă toate domeniile im-

portante; astfel, în timp, ele devin un depozit de experienţă pentru funcţia de audit.
Un alt aspect important este acela că aceste chestionare nu trebuie proiectate chiar în timpul procesului de audit: numai completarea lor şi evaluarea chestionarelor completate trebuie făcută în timpul auditului. Completarea şi evaluarea chestionarelor ar trebui făcută chiar la începutul auditării, pentru a da indicaţiile necesare auditorilor asupra zonelor în care trebuie să-şi concentreze atenţia.
Este foarte important ca un auditor care completează şi evaluează un CCI să înţeleagă semnificaţia întrebărilor conţinute şi posibilele implicaţii ale răspunsurilor nesatisfăcătoare date la anumite întrebări. În plus, în cadrul acestei tehnicii, auditorul actionează pe ghicite în multe aspecte, lucru care face tehnica dificil de utilizat. Ea nu indică cu precizie despre ce risc sau riscuri este vorba când se face referire la o anumită cheie de control.
Chestionarul nu reliefează faptul că unul sau mai multe controale se referă la acelaşi risc, şi nici cazurile în care aşa-numitele controale la care se referă o întrebare nu sunt legate de nici un risc anume (controlul fiind redundant).
Tehnica chestionarului nu permite diferenţierea controalelor din punctul de vedere al eficacităţii lor, chiar dacă funcţionează corespunzător: unele controale sunt potenţial mai bune (eficace) decât altele. În plus, tehnica CCI nu permite decât răspunsuri "da" şi "nu", eventual cu posibilitatea ca auditorul să adauge o observaţie, în timp ce în realitate, nu există satisfacere deplină sau nesatisfacere de loc a controalelor - satisfacerea poate fi parţială şi satisfacerea parţială este mai bună decât nesatisfacerea controalelor.
Chestionarele de control intern constituie un instrument inexact, care poate fi cu succes înlocuit cu o tehnică bazată pe o matrice de control, având ca suport un program de calcul tabelar. Această tehnică înlătură în mare măsură dezavantajele tehnicii CCI.

Tehnica matricei de control

Matricea de control seamănă în multe aspecte, cu descrierea făcută pentru CCI. Completarea şi evaluarea matricei are loc în timpul auditului, dar, cu excepţia unui singur pas, toţi ceilalţi paşi sunt realizaţi cu ajutorul calculatorului. Matricea de control completată şi evaluată este un excelent mijloc de autodocumentare în timpul auditului. Spre deosebire de CCI, evaluarea matricei de control completate este o parte integrantă a tehnicii; totuşi, auditorul nu este obligat să accepte interpretarea matricei de control dată de calculator. Ca şi pentru CCI, este bine ca matricea să fie completată şi evaluată la începutul auditului, pentru a ghida echipa în repartizarea timpului rămas.
În tehnica matricei de control, se utilizează axa orizontală a unei foi de calcul pentru a memora expunerile la risc şi axa verticală pentru a memora controalele. *O expunere la risc* este o consecinţă sau un rezultat pe care organizaţia încearcă să-l evite. *Un control* este o procedură sau o măsură care reduce sau elimină probabilitatea ca una sau mai multe expuneri la risc să apară.
Rezultatul final al tehnicii este atribuirea unui punctaj fiecărei expuneri la risc, în funcţie de gravitatea ei şi de gradul în care este ţinută sub control. Acest punctaj este numit *grad de expunere*. Se va folosi o scală cu patru nivele, de la 1 la 4. Echipa de audit va trebui să-şi aloce majoritatea timpului domeniilor celor mai expuse (având gradul 4). Dimpotrivă, celor cu gradul 1 nu li se va acorda nici o importanţă, pentru că ele nu reprezintă de fapt nici o expunere la risc.
Tehnica este valabilă şi dacă auditorul înlocuieşte expunerile cu obiective şi

controalele cu măsuri. Totuşi, în descrierea tehnicii dată în continuare, se presupune că auditorul lucrează în modul preventiv, unde expunerile şi controalele constituie "modus operandi". Recomandarea este ca auditorii să încerce să folosească tehnica, făcând uz de un minim de expuneri si controale. Un număr prea mare din oricare dintre ele îl sufocă pe auditor cu prea multe detalii şi îl îndepărtează de la viziunea tabloului general al riscurilor.

Diferențierea riscurilor inerente

O expunere poate să nu fie intrinsec la fel de gravă ca o alta, indiferent de gradul relativ de control asupra fiecăreia dintre ele. Există diferite grade de risc inerent pentru diferitele expuneri, şi această tehnică matriceală, spre deosebire de tehnica CCI, poate ține cont de ele. Se sugerează că riscul inerent al unei expuneri poate fi determinat suficient de precis, luând în considerare categoria şi dimensiunea sa probabilă; şi nivelul calculat al acestuia este înscris pe prima linie a tabelului, în dreptul fiecărei expuneri. Atât categoria, cât şi dimensiunea, sunt determinate la proiectarea matricei, înainte de începerea auditului propriu-zis.

Categorii de risc

Compartimentele de audit trebuie să verifice dacă abordarea standard propusă este potrivită pentru scopurile urmărite de ele, sau dacă trebuie să o "ajusteze" mai precis pentru condițiile lor specifice. Se recomandă ca stabilirea categoriei din care face parte expunerea să fie determinată prin estimarea nivelului maxim care poate fi atins de această expunere. Să presupunem că avem o scală cu 6 nivele , cu nivelul maxim 6. Pentru o expunere anume, parcurgem scala şi vedem care este nivelul maxim care poate fi atins. Acesta va fi considerat ca fiind nivelul categoriei. Fiecare compartiment de audit îşi poate proiecta propria scală de categorii, consultându-se cu managementul general, în aşa fel încât să reflecte filozofia şi nevoile organizației. Ca punct de plecare, oferim următoarele scale de categorii, pentru situațiile când tehnica se foloseşte în contextul obiectivelor sau expunerilor. Cu cât nivelul atins este mai înalt, cu atât este potențial mai important respectivul obiectiv sau expunere.

SCARA DE CLASIFICARE (OBIECTIVE)

Nivel (cel mai înalt)	6	Conducerea trebuie să înțeleagă ce se petrece la nivelul întregii organizații şi să se poată adapta corespunzător
	5	Obiectivele globale pe termen mediu-lung trebuie îndeplinite
	4	Trebuie atinse valorile propuse legate de buget şi profit
	3	Conducerea trebuie să acționeze adecvat pentru a corecta funcționarea
	2	Conducerea trebuie să înțeleagă ce se petrece la nivelele funcționale
(scăzut)	1	Trebuie să existe o motivație puternică

SCARA DE CLASIFICARE (EXPUNERI LA RISC)

Nivel (cel mai înalt)	6	Pierdere de informaţii
	5	Scăderea numerarului sau a altor bunuri sau creşterea datoriilor
	4	Pierderea sau periclitarea reputaţiei
	3	Micşorarea sau exagerarea profitului
	2	Distorsionarea bilanţului
(scăzut)	1	Eroare contabilă cu afectarea declaraţiei de profit şi pierdere sau a bilanţului

Dimensiunea riscului

Scara de clasificare nu este suficientă pentru a reliefa importanţa relativă a obiectivelor şi expunerilor. De exemplu, o anumită expunere la risc poate prezenta riscul unei pierderi de informaţii, dar într-un mod oarecare, se cunoaşte faptul că e improbabil ca pierderea de informaţii să fie de mare întindere. Pe de altă parte, aceeaşi expunere poate risca o foarte mare cantitate de bani numerar. Deci, trebuie ca dimensiunea să fie luată în considerare şi tehnica propune ca acest lucru să se facă în partea superioară a coloanelor tabelei, folosind pentru fiecare expunere următoarele aproximări :

3	mare/foarte sensibil/ critic/ preponderent material
2	mediu/sensibil/material
1	mic/ insensibil/ necritic/ nematerial

Categoria şi dimensiunea combinate

Este improbabil să se noteze un obiectiv sau o expunere în perfectă concordantă cu nivelul maxim probabil. Aşa încât se va utiliza nivelul cel mai înalt al categoriei, care, împreună cu cea mai mare valoare a dimensiunii riscului, dă cel mai mare rezultat compus. Tehnica recomandă înmulţirea categoriei cu dimensiunea, astfel încât o potenţială pierdere mare de numerar (3x5) va produce un rezultat mai mare decât o potenţială pierdere medie de informaţii (2x6).

Reflectarea gradului de control în matrice

În celula unde o anume expunere intersectează un anumit control, se va introduce o valoare a gradului în care controlul este considerat eficace în reducerea sau eliminarea expunerii. Tehnica cere ca matricea să fie proiectată în aşa fel încât la fiecare intersecţie a unei expuneri cu un control, să poată fi inserate trei valori:

- nivelul ideal al controlului;
- nivelul de respectare a controlului;
- nivelul real al controlului.

Se recomandă ca aproximarea fiecăreia din cele trei să se facă cu valori de la 0 (cel mai slab) la 5 (cel mai bun).

Nivelul ideal al controlului (I)

Atunci când se face proiectarea matricei pentru un anumit domeniu de activitate (de obicei nu în timpul auditului propriu-zis, ci înainte), se face o apreciere a nivelului (proporţiei) în care se poate aştepta ca un anumit control să reducă sau chiar să elimine în întregime o anume expunere în condiţii ideale - adică atunci când acesta funcţionează exact cum s-a intenţionat la proiectarea lui. Acest nivel este introdus în tabel ca nivel ideal. Pentru

fiecare control, se atribuie un nivel în raport cu fiecare expunere pe o scară de la 0 (*'controlul nu are impact asupra expunerii'*) şi până la 5 (*'controlul elimină complet expunerea'*). Tabelul trebuie proiectat astfel încât nivelul implicit să fie 0 (dacă nu se introduce altă valoare).
Aceste valori fiind introduse la crearea matricei, echipa de audit le va putea modifica în timpul auditului dacă acest lucru devine necesar. În realitate, din când în când echipa de audit modifică aceste valori în lumina experienţei. Compartimentul de audit poate, de asemenea, opera adăugări, modificări şi ştergeri asupra expunerilor şi controalelor în lumina experienţei acumulate, aşa încât matricea să devină, an după an, un instrument mai bun.

Nivelul de respectare a controlului (de conformare - C)

Chiar la începutul auditului, echipa de audit introduce un nivel de respectare, pe scara de la 0 la 5, exprimând proporţia în care echipa consideră că este respectat în practică fiecare control din matrice. Cantitatea de teste de audit necesare pentru a lua o decizie în privinţa nivelului este o problemă de politică de audit şi poate varia în funcţie de împrejurări. Este de preferat un minimum de teste şi folosirea, în completare, a documentării, manualelor de proceduri şi discuţiilor cu personalul de specialitate. Este inadecvat să se consume prea mult timp cu testele în această etapă a auditului, de vreme ce tehnica este menită tocmai să direcţioneze efortul de audit ulterior către anumite domenii "sensibile". Trebuie introdus un singur nivel , într-o singură celulă, pentru fiecare control existent în matrice. Automat, se va insera aceeaşi valoare în toate celulele, pentru fiecare expunere care depinde de acest control, pentru a fi redusă sau eliminată. Dacă axa verticală este folosită pentru măsuri în loc de controale, se testează eficacitatea în locul respectării.

Nivelul real al controlului (R)

Acest nivel este calculat automat, din nivelul ideal şi cel de conformitate. Dacă, de exemplu, un control ar reduce o expunere într-o anumită măsură, dacă ar funcţiona aşa cum a fost proiectat tot timpul (nivelul ideal), dar studiul referitor la respectare făcut de auditori arată că nu este întotdeauna respectat (nivelul de respectare), aceste două mărimi pot fi combinate pentru a arăta proporţia în care controlul, aşa cum este el respectat, reduce într-adevăr expunerea la risc (nivelul real al controlului). Nivelul real se obţine prin scăderea inversului nivelului de respectare a controlului din nivelul ideal. Inversul este obţinut din următorul tabel:

Nivel de respectare	0	1	2	3	4	5
Inversul nivelului	5	4	3	2	1	0

Combinarea unui număr de nivele de control

Matricea a fost proiectată astfel încât fiecare expunere să aibă o coloană separată. În cadrul acestei coloane pot exista înscrise unul sau mai multe nivele reale. Dacă există trei controale care influenţează expunerea, atunci vor fi trei nivele reale ale controalelor în coloana acestei expuneri.

Categorie, dimensiune şi nivele de control combinate

Pentru a obţine gradul de expunere (GE) (pe o scară de la '1' la '4') pentru o expunere sau un obiectiv, se vor combina nivelul categoriei şi dimensiunii dintr-o coloană , cu nivelul combinat de control. Reamintim că nivelurile categoriilor se plasează pe o scară de la 1 la 6 (cel mai grav) şi

dimensiunile pe o scară de la 1 la 3 (cea mai mare). Formula folosită pentru a combina toate aceste informații este:

Ca x D x (125 - Co) > 1500		GE = 4	unde:
	> 751 şi <1500	GE = 3	Ca = categoria
	> 1 şi <750	GE = 2	D = dimensiunea
	<= 0	GE = 1	Co = suma cuburilor nivelurilor reale ale controalelor de pe coloană

Grade de expunere

Interpretarea gradelor de expunere se poate face astfel:

GE= 4 Un domeniu de audit potențial foarte important, care poate necesita o activitate considerabilă pentru atingerea obiectivelor auditului.

GE=3 O activitate de audit ar fi justificată, dacă timpul o permite.

GE=2 Este improbabil ca activitatea de audit să fie justificată, datorită riscului relativ scăzut în acest domeniu.

GE=1 Gradul de siguranță al auditului în raport cu acest risc potențial este deja adecvat.

Un exemplu

Exemplul de mai jos este o matrice construită pentru rețeaua locală de calculatoare a unei firme mici. Obiectivele şi măsurile sunt enumerate pe axa orizontală, respectiv verticală. Obiectivele sunt enumerate în Tabelul 1. Tabelul 2 prezintă matricea la începutul auditului. Valorile pe scara de clasificare şi respectiv dimensiunea au fost deja determinate, ca şi proporția în care este de aşteptat ca fiecare măsură să contribuie la atingerea fiecărui obiectiv (nivelurile ideale, I). În acest stadiu, gradul de expunere este calculat provizoriu, bazându-se doar pe valorile S, D şi I, neexistând valori pentru C şi R. Dacă perioada de timp consacrată auditului este scurtă, echipa de audit poate hotărî să nu mai testeze eficacitatea măsurilor care sunt legate doar de obiective cu un grad de expunere mai mic ca 3.

Tabelul 3 arată rezultatele după introducerea valorilor care indică eficacitatea (sau respectarea) controalelor în liniile C ale tabelului în timpul stadiilor de început ale auditului. Auditorii îşi vor concentra în mare parte timpul obiectivelor cu un grad de expunere de 4 sau 3.

De subliniat că acesta este doar un exemplu general, de principiu. Obiectivele şi măsurile, precum şi valorile respective pot să nu fie aplicabile în nici o organizație anume; totuşi, el are meritul de a prezenta tehnica "la lucru".

Tabelul 1. TITLUL (obiectivului sau expunerii)

A	Disponibil 100% pentru toți utilizatorii
B	Utilizatorii înteleg şi folosesc toate caracteristicile sistemului
C	Sistemul oferă o gestionare adecvată a informațiilor
D	Sistemul respectă cerințele funcționale
E	Sistemul are o interfață utilizator prietenoasă
F	Se întreţin baze de date intercorelate
G	Este asigurată securitatea datelor şi informațiilor
H	Este asigurată securitatea software-ului
I	Este asigurată securitatea hardware-ului
J	Există potențial pentru dezvoltări viitoare ale sistemului

Tabelul 2

			OBIECTIVE/EXPUNERI LA RISC									
			A	B	C	D	E	F	G	H	I	J
Gradul de expunere calculat	**(GEC)**		3	2	4	3	2	4	4	3	2	4
Categoria(6 este limita superioară)	**(S)**		4	2	6	4	3	6	6	4	4	5
Dimensiunea(3 este lim. superioară)	**(M)**		2	2	3	3	2	3	3	2	1	3
MĂSURI/CONTROALE												
1. Există un program eficient de instruire pt.utilizatori	(I)			4		3	3		3	3		
	(C)	?		?		?	?		?	?		
	(R)											
2.Controlul funcționării sistemului se face regulat și este eficace	(I)		4			3						
	(C)	?	?			?						
	(R)											
3. Se utilizeaza doar hardware și software de calitate (care respectă standardele)	(I)		3	2			4	2		3	3	3
	(C)	?	?	?			?	?		?	?	?
	(R)											
4. Există asigurari încheiate pentru riscurile semnificative care nu pot fi reduse în alt mod	(I)								5			
	(C)	?							?			
	(R)											
5. Cerințele utilizatorilor sunt definite cu atenție	(I)		3	4	3		4	2	2			2
	(C)	?	?	?	?		?	?	?			?
	(R)											
6. Există documentație completă ținută pentru toate sistemele și aceasta e la zi	(I)		3		3			4				3
	(C)	?	?		?			?				?
	(R)											
7. Condițiile de cumpărare a licenței de soft sunt cunoscute și respectate	(I)			2						4		
	(C)	?		?						?		
	(R)											
8. Se dispune de un stoc de piese de schimb și întreținerea este asigurată de personal propriu	(I)		3			3					4	
	(C)	?	?			?					?	
	(R)											
9. Exista o evidență centralizată a hardului și softului	(I)							2		2	2	2
	(C)	?						?		?	?	?
	(R)											
10.Planificarea dezvoltării viitoare a funcției informatice este facută în contextul planificării de ansamblu	(I)							3				3
	(C)	?						?				?
	(R)											
11.Se creează și se păstrează în siguranță copii ale programelor și fișierelor de date	(I)		2					2	5	5		
	(C)	?	?					?	?	?		
	(R)											
12.Managerii coordonează auto-auditări adecvate ale sistemelor lor de TI	(I)		2	2	2	2	2	2	2	2	2	2
	(C)	?	?	?	?	?	?	?	?	?	?	?
	(R)											

Tabelul 3

			OBIECTIVE/EXPUNERI LA RISC									
			A	B	C	D	E	F	G	H	I	J
Gradul de expunere calculat	**(GEC)**		2	2	4	3	2	3	1	2	2	3
Categoria(6 este limita superioară)	**(S)**		4	2	6	4	3	6	6	4	4	5
Dimensiunea(3 este lim. superioară)	**(D)**		2	2	3	3	2	3	3	2	1	3
MĂSURI/CONTROALE												
1. Există un program eficient de instruire pt.utilizatori	(I)			4		3	3		3	3		
	(C)	4		4		4	4		4	4		
	(R)			3		2	2		2	2		

2.Controlul funcționării sistemului se face regulat și este eficace	(I)			4			3						
	(C)		5	5			5						
	(R)			4			3						
3. Se utilizeaza doar hardware și software de calitate (care respectă standardele)	(I)			3	2			4	2		3	3	3
	(C)		2	2	2			2	2		2	2	2
	(R)							1					
4. Există asigurari încheiate pentru riscurile semnificative care nu pot fi reduse în alt mod	(I)									5			
	(C)		5							5			
	(R)									5			
5. Cerințele utilizatorilor sunt definite cu atenție	(I)			3	4	3		4	2	2			2
	(C)		3	3	3	3		3	3	3			3
	(R)			1	2	1		2					
6. Există documentație completă ținută pentru toate sistemele și aceasta e la zi	(I)			3		3			4				3
	(C)		4	4		4			4				4
	(R)			2		2			3				2
7. Condițiile de cumpărare a licenței de soft sunt cunoscute și respectate	(I)				2						4		
	(C)		2		2						2		
	(R)										1		
8. Se dispune de un stoc piese de schimb și întreținerea este asigurată de personal propriu	(I)			3			3					4	
	(C)		2	2			2					2	
	(R)											1	
9. Există o evidență centralizată a hardului și softului	(I)								2		2	2	2
	(C)		5						5		5	5	5
	(R)								2		2	2	2
10.Planificarea dezvoltării viitoare a funcției informatice este facută în contextul planificării de ansamblu	(I)								3				3
	(C)		4						4				4
	(R)								2				2
11.Se crează și se pastrează în siguranță copii ale programelor și fișierelor de date	(I)			2					2	5	5		
	(C)		3	3					3	3	3		
	(R)									3	3		
12.Managerii coordonează auto-auditări adecvate ale sistemelor lor de TI	(I)			2	2	2	2	2	2	2	2	2	2
	(C)		4	4	4	4	4	4	4	4	4	4	4
	(R)			1	1	1	1	1	1	1	1	1	1

Concluzii

Tehnica descrisă recomandă folosirea unei matrice de control bazată pe utilizarea unui program de calcul tabelar, care să informeze echipa de audit unde să-și aloce timpul. Timpul de audit este alocat în concordanță cu riscurile relative asociate fiecărei coloane a matricei. Pe coloană se pot plasa fie expuneri la risc, fie obiective, în funcție de alternativa aleasă de echipa de audit, de a pune accentul în audit pe ceea ce ar putea să meargă rău, sau pe ceea ce trebuie urmărit de către manageri.

Bibliografie

1. Frederick Gallegos, Dana R Richardson, A. Faye Borthick - *Audit and Control of Information Systems*, South-Western Publishing Co, Ohio, 1987
2. Andrew D.Chambers, John M.Court - *Computer Auditing*, Pittman Publishing, London, UK, 1991
3. Ian Douglas - *Computer Audit & Control Handbook*, Butterworth and Heinemann, Oxford, UK, 1995
4. Etienne Barbier - *L'audit interne*, Les Editions d'Organisation, 1989
5. J.S.R Venables - *Internal Audit*, Butterworth and Heinemann, 1991
K.W.Impey.