Risk Assessment Generated by Usage of ICT and Information Security Measures

Prof.dr. Ilie Tamaş
ASE Bucureşti

Information societies involve the usage of information technology and communications (ITC) on a large scale. The dependence on ITC is an unquestionable problem in the present, because we assist to a generality of computers usage in all economic and social life activities. That is why organization information systems became accessible at the global level and there are permanently open for a quick exchange of information between different categories of users located by different geographical nods. The ITC usage involves the existing of some risks that should be known, evaluation and based on these, we must have information systems security measure. We consider that the risk is an indicator very important that must be permanently assess in the usage process of the information system based on ITC. Risk management suppose a permanently evaluation of these problems and also restrain by some practical actions who goes to the decrease of its effects. From the expose point of view, in this paper work it is presented the results of research based on specialty literature and current cases from practical activities, regarding the risks of ITC usage and their diminishing measure. There are distinguished the main factors (threat, vulnerability and impact) who affect the information risk and on the other way, diminishing measure of the action to these factors for optimum working of an economic and social organism who use ITC. We consider that through proposed measures we assume safety in design process, implement and usage of the informational systems based on ITC.

Keywords: *information and communications technology, (ICT), risk assessment, , impact, vulnerability, information security, protection measures.*

I. INTRODUCERE

În cadrul organizațiilor economice şi sociale se utilizează în prezent pe scară largă tehnologiile informaționale şi de comunicații (TIC).

Dezvoltarea TIC oferă un acces la o mare cantitate de informații, care poate fi cercetată din diverse puncte de vedere şi utilizată în procesele decizionale de către diferite categorii de utilizatori, atât la nivel microeconomic cât şi macroeconomic.

Dependența de tehnologiile informaționale este un factor cheie in societatea actuală in care generalizarea utilizării calculatorului electronic în domeniul economic şi social stă la baza utilizării principiilor şi metodelor moderne de management.

Utilizarea TIC ridică însă probleme deosebite pentru manageri, utilizatori, proiectanți şi alte categorii implicate în activitățile desfăşurate, deoarece aceste tehnologii presupun anumite riscuri în procesul de utilizare. Dezvoltarea serviciilor INTERNET a adus o vulnerabilitate şi mai mare, apărând o diversificare a riscurilor.

II. TIPURI DE RISCURI şi măsuri de protecție

Riscurile conduc la creşterea potențialului de apariție a erorilor si activităților frauduloase în aplicații, baze de date, fişiere sau activități de procesare, ca urmare, este nevoie sa fie monitorizate permanent cu scopul de a produce efecte minime. Riscurile respective trebuie identificate, cunoscute şi evaluate pentru a se lua toate măsurile necesare în vederea contracarării lor. Ca şi în alte domenii şi în TIC din punct de vedere al posibilității de a se produce, există riscuri potențiale şi riscuri posibile. **Riscurile potențiale** sunt cele mai susceptibile de a se produce, de aceea, ele trebuie identificate şi corectate, iar **riscurile posibile** sunt o parte a riscurilor potențiale, în care există o anumită probabilitate ca anumi-

te erori să se producă fără să fie detectate şi corectate. Rezultă că toate tipurile de riscuri ce planează în procesul de utilizare a TIC, precum şi procedurile de asigurare a securităţii informaţiilor necesită toată atenţia din partea proiectanţilor de sisteme informatice precum şi a factorilor decizionali din întreprinderea sau organizaţia utilizatoare.

În urma cercetărilor efectuate pe baza literaturii de specialitate, precum şi a situaţiilor concrete din întreprinderile care utilizează TIC s-a ajuns la concluzia că din punct de vedere al specificului activităţilor TIC, riscurile pot fi grupate aşa cum rezultă din figura 1.

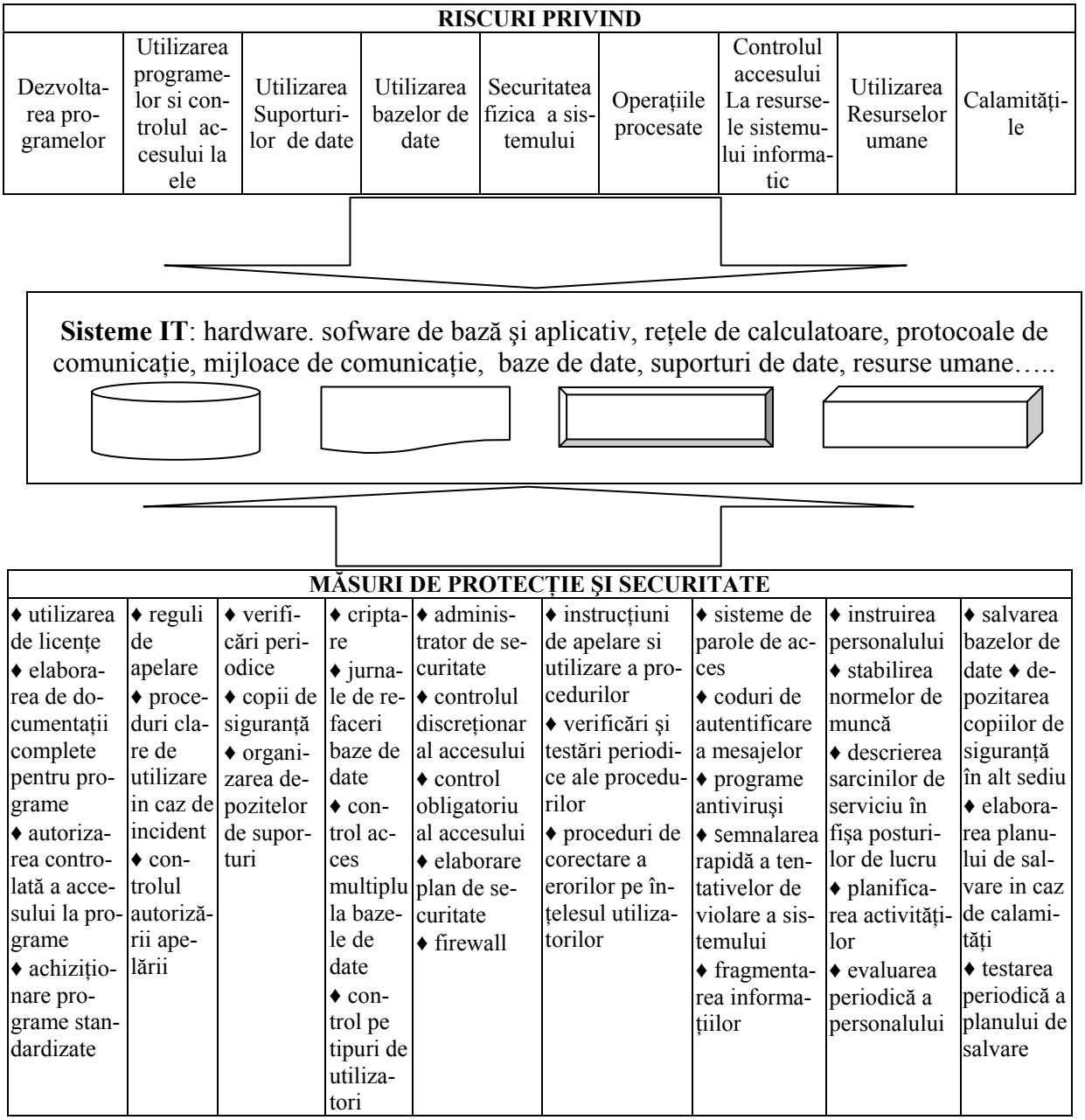

Fig.1. Tipuri de riscuri privind TIC, măsuri de securitate şi protecţie

Considerăm că această clasificare permite o ordonare mai bună a măsurilor de protecţie şi securitate a informaţiilor, precum şi o evaluare mai reală a riscurilor TIC.

În cele ce urmează vom prezenta o sinteză a cercetărilor noastre cu privire la tipurile de riscuri privind sistemele ce utilizează TIC şi ce implicaţii are fiecare tip de risc, precum şi măsurile de protecţie şi securitate ce se im-

pun pentru diminuarea acțiunii lor, sau uneori anihilarea totală a efectelor negative ale acestora, astfel:

☎ ***Riscurile privind dezvoltarea programelor de aplicații*** se referă la:

- faptul că pot apărea erori de programare ce nu au fost depistate în procesul testării si implementării lor, sau pe parcursul utilizării programului respectiv a intervenit un programator sau utilizator neautorizat, realizând unele modificări care nu răspund in totalitate cerintelor de prelucrare;
- lipsa documentației tehnice de proiectare şi realizare;
- utilizarea de soft şi hard neautorizate;
- schimbări necontrolate în mediul economic sau social;

Măsurile de protecție şi securitate se referă la:

- existența licențelor pentru toate programele utilizate;
- specificarea clară a posibilităților de dezvoltare a programelor de către proiectanți sau de către utilizatori;
- existența unei documentații complete cu privire la programele utilizate;
- achiziționarea unor programe standardizate şi limitarea modificărilor la minim necesar;

☎ ***Riscurile privind utilizarea programelor şi controlul accesului la acestea*** se referă la apariția unor erori in procesul de utilizare a programelor de aplicații, ca urmare a nerespectării secvențelor de apelare a modulelor, procedurilor, formatelor corespunzătoare si a altor parametrii.

În acest caz se pot întâmpla:

- pierderi de date ca urmare a unor incidente in funcționarea sistemului;
- eşuarea unor tranzacții individuale;
- erori in introducerea datelor;
- inițieri automate ale unor operații care nu sunt vizibile si care devin greu de controlat;

Măsurile de protecție şi securitate se referă la:

- reluarea execuției procedurilor în caz de incidente;
- existenta unor proceduri clare de validare a datelor;
- prevederea unor puncte de reluare a prelucrărilor;
- controlul sever al accesului autorizat la programe.

☎ ***Riscurile legate de utilizarea suporturilor de date*** se referă la:

- deteriorarea suporturilor de date;
- deteriorarea mecanismelor de citire/scriere a suporturilor;
- furturi de suporturi de date.

Măsurile de protecție şi securitate se referă la:

- efectuarea periodică a unor copii de siguranță;
- controlul permanent al accesului personalului autorizat în depozitul de suporturi de date;
- organizarea corespunzătoare a depozitelor de suporturi de date .

☎ ***Riscurile privind utilizarea bazei de date*** se referă la:

- pierderi de date ca urmare a unor incidente in funcționarea sistemului;
- eşuarea unor tranzacții individuale;
- manipularea neautorizată a datelor şi informațiilor;
- căderea locală a sistemului ca urmare a întreruperii alimentării cu curent electric;
- distrugerea intenționată sau neintenționată a bazei de date.
- violarea securității datelor.

Măsurile de protecție şi securitate se referă la:

- refacerea bazei de date după ce a avut loc o eşuare sau o distrugere având în vedere informațiile stocate redundant în altă parte a sistemului, precum şi existența unor puncte de salvare şi reluare;
- existența unor jurnale de refaceri în care sunt înregistrate toate detaliile actualizării înainte şi după executarea actualizării respective;
- reîncărcarea sistemului de operare şi reluarea operațiilor eşuate;
- controlul accesului multiplu la baza de date prin intermediul unor tehnici speciale cum sunt: blocajele partajate sau exclusive, serializarea, izolarea, gruparea, etc.;
- întocmirea unor planuri de recuperare a datelor;

- controlul accesului la baza de date pe tipuri de utilizatori.

☎ ***Riscuri privind securitatea fizică a sistemului informațional*** se referă la:
- accesul neautorizat la hard si soft;
- gestionarea necorespunzătoare a sistemului de operare;
- dezvoltarea neautorizată a programelor;
- violarea securității spațiului unde se află echipamentele, programele, informațiile;
- calamități naturale(cutremur, inundație, incendiu etc.) ;
- căderi de hardware/software;

Măsurile de protecție şi securitate în acest caz se referă la:
- numirea unui administrator de securitate;
- controlul discreționar al accesului;
- controlul obligatoriu al accesului;
- elaborarea unui plan de securitate;
- criptarea datelor;
- firewall.

☎ ***Riscuri legate de operațiile procesate*** se referă la:
- utilizarea necorespunzătoare a programelor;
- codificări eronate ale operațiilor care nu au fost depistate în procesul de testare a programelor şi a sistemului în ansamblul său;

Măsurile de protecție şi securitate în acest caz se referă la:
- existența unor instrucțiuni clare pentru apelarea procedurilor de prelucrare;
- proceduri de corectare a erorilor pe înțelesul utilizatorilor;
- depistare erorilor de programare încă din etapa de implementare a programelor;

☎ ***Riscurile privind controlul accesului la resursele unui sistem informatic*** se referă la:
- acces neautorizat la resursele sistemului;
- furturi de fişiere sau baze de date;
- virusarea fişierelor, programelor, etc.

Faptul că în prezent prin intermediul rețelei INTERNET orice utilizator individual poate avea acces la un volum mare de informații, unele dintre acestea fiind confidențiale şi de importanță deosebită, trebuie luate măsuri de protecție pentru asigurarea unui control total la resursele sistemului.

Pentru controlul accesului la resursele respective se utilizează:
- un sistem de parole de acces pentru diferite categorii de utilizatori;
- coduri de autentificare a mesajelor;
- protejarea programele de bază şi de aplicații, fişierele, bazele de date prin programe de detectare a virusilor informatici şi de distrugere a acestora;
- controlul permanent al accesului în sălile unde sunt amplasate echipamentele si mai ales serverele;
- copii de siguranță pentru programe şi bazele de date, care trebuie păstrate in altă parte decât unde este sediul organizației care utilizează TIC;
- semnalarea rapidă şi eficientă a tentativelor de violare a sistemului respectiv;
- eliminarea posibilităților ascunse de a deduce anumite informații din baza de date.
- utilizarea semnăturii digitale;
- fragmentarea informațiilor transmise pentru limitarea impactului de agresiune.

☎ ***Riscurile legate de utilizarea resurselor umane*** se referă la:
- erori si omisiuni de date cauzate de personalul angajat;
- fraude;
- pregătirea necorespunzătoare a personalului;

Reducerea acestor riscuri se realizează printr-o serie de proceduri bine stabilite cu privire la:
- instruirea personalului in conformitate cu cerințele impuse de evoluția TIC si cu planul general de utilizare a acestor tehnologii;
- stabilirea corespunzătoare a normelor de muncă;
- descrierea clară a sarcinilor de serviciu pe posturi de lucru şi consemnarea lor în fişele de post;
- planificarea activităților pe fiecare persoană implicată în sistem;
- organizarea locurilor de munca in domeniul TIC şi planificarea periodică a activităților pe fiecare persoană;
- evaluarea periodică a personalului pe baza unor criterii ce au in vedere instruirea, experiența, gradul de responsabilitate, sarcinile executate precum si alte aspecte.

☎ ***Riscuri legate de calamități*** se referă în principal la:

- cutremure;
- incendii;
- inundaţii, etc.

Pentru prevenirea acestor riscurile se vor elabora planuri de recuperare pentru situaţii de calamitate în care se va prevedea executarea unor proceduri cum sunt:

- salvarea fişierelor si a bazelor de date si depozitarea lor in alt loc decât sediul organizaţiei respective, eventual în altă localitate;
- efectuarea actualizării salvărilor după un grafic stabilit foarte riguros;
- testarea la anumite intervale a procedurilor de salvare si restaurare a fişierelor si a bazelor de date;
- testarea generală a planului de continuitate a activităţilor in caz de calamităţi, care să permită efectuarea operaţiilor curente in cadrul organizaţiei respective si sa existe documente elaborate in acest scop.

Evaluarea riscurilor referitoare la utilizarea TIC trebuie să aibă în vedere importanţa informaţiilor obţinute şi vehiculate în sistemul respectiv, identificarea punctelor vulnerabile, şi pe această bază elaborarea unei strategii de securitate. Analiza situaţiilor de risc şi cuantificarea lor se realizează plecând de la potenţialitatea riscurilor şi impactul produs de acestea asupra sistemului respectiv.

Suntem de aceeaşi părere exprimată în (2SI Sécurité des Systemes d'Information - Mehari et le management de la sécurité sept.2002), conform căreia ***potenţialitatea unui risc*** reprezintă probabilitatea de apariţie a lui, iar ***impactul*** este dat de gravitatea consecinţelor directe şi indirecte ce decurg din apariţia riscului respectiv.

Potenţialitatea şi impactul riscului depind în mod direct de măsurile de securitate ce au fost adoptate în cadrul organizaţiei respective.

Evaluarea riscului TIC din punct de vedere cantitativ se realizează plecând de la o analiză detaliată a vulnerabilităţii şi a impactului produs asupra sistemului, precum şi de potenţialitatea riscurilor respective. Fiecărui nivel de risc i se poate asocia o probabilitate de producere, iar pe această bază se realizează o scară de valori de disfuncţii provocate ca urmare a producerii unor evenimente datorate riscului.

Metodologia propusă de MEHARI[1] utilizează o scară cu 4 niveluri de gravitate a disfuncţiilor provocate de riscuri şi anume:

nivelul 1 – nesemnificativ, în care impactul asupra rezultatelor este foarte mic sau de neluat în seamă;

nivelul 2 – important, aici perturbaţiile în sistem sunt notabile, trebuie avute în vedere, dar sunt suportabile;

nivelul 3 - grav, în care disfuncţiile sunt grave la nivelul organizaţiei, iar unele activităţi pot fi compromise;

nivelul 4 - *vital,* unde disfuncţiile sunt extrem de grave, existând pericolul ca organizaţia sau părţi din aceasta să nu mai existe.

Aceste niveluri se pot utiliza pentru elaborarea unor scenarii privind disfuncţiile produse şi a unei scări de valori a lor cu privire la organizaţia studiată.

De exemplu *evaluarea riscurilor TIC privind un sistem informatic de evidenţă şi urmărire a aprovizionării cu materii prime a unei întreprinderi* se poate realiza construind un scenariu aşa cum rezulta din tabelul 1.

Tabel 1.

DISFUNCTII	Nivel 1 Nesemnificativ	Nivel 2 Important	Nivel 3 Grav	Nivel 4 Vital
Incapacitate de aprovizionare cu materii prime datorată deteriorării bazei de date	Incapacitate < 6 ore	Incapacitate între 6 ore si 3 zile	Incapacitate peste 3 zile	Incapacitate > 6 zile
Deteriorarea terminalului de la magazia de materiale	<1oră	< 5 ore	Peste 1 zi	
Stocuri neactualizate ca urmare a unei virusări	< 2 ore	< 4 ore	Peste 1 zi	
.....	.....	.....	.....	.....

Scenariul poate fi continuat şi cu alte exemple. La nivel de organizaţie se construiesc scări cu valoarea disfuncţiilor pentru toate activităţile, se reunesc apoi, obţinându-se o

situație sintetică relevantă pentru o perioadă dată. Pe baza acesteia se pot efectua estimări financiare cu privire la riscuri, ceea ce aduce un plus de informații în cadrul tabloului general despre riscurile TIC. În acest scop este necesară o identificare a tuturor perturbațiilor şi disfuncțiilor produse, precum şi a cauzelor care le determină, iar pe această bază luarea măsurilor de protecție corespunzătoare după caz, aşa cum au fost prezentate anterior în lucrare.

În urma cercetările efectuate a rezultat că *gestionarea riscurilor într-un mediu ce utilizează TIC* impune efectuarea în permanență a unor controale eficiente referitoare la:

- elaborarea unor planuri de securitate a informațiilor;
- proiectarea, dezvoltarea si întreținerea sistemelor informatice;
- existența unor conformități cu standardele interne şi externe în domeniu;
- asigurarea integrității şi confidențialității datelor;
- existența unor documente şi planuri privind continuarea activității în cazuri de calamități, dezastre, etc.;
- accesul şi securitatea fizică si logică la rețele de calculatoare;
- protecția împotriva utilizării softului neautorizat;
- securitatea fizică a site-lor organizației;
- protecția fizică a componetelor sistemului, etc.;
- auditarea sistemului informațional şi altele.

De asemenea, riscurile legate de atitudinea conducerii față de utilizarea TIC au o importanță deosebită, deoarece au in vedere faptul ca managerii pot ignora anumite riscuri, după cum în acelaşi tip pot utiliza proceduri de control intern detaliate pentru prevenirea si diminuarea altor categorii de riscuri.

III. Concluzii

Managementul modern trebuie să fie sensibil față de riscuri, să urmărească implementarea si utilizarea unor sisteme TIC fiabile si performante, elaborând în acest scop planuri de acțiune şi scheme de securitate cu ierarhizarea obiectivelor pe nivele operaționale adaptabile la schimbările care apar în permanență.

Bibliografie

C. J. Date (2004), - Baze de date, 8 Edition, Editura E+

Hawley, J., Green, P. (2002) - Capitalisation of Software, Audit Report No. 54 -03

Popa Ş., Ionescu, C. (2005) - Auditul în medii informatizate, Editura Expert, Bucuresti

(2005) Report of the best practics and metrics team, corporate information Security Working Group, Subcommitte on Technology, Information Policy, Intergovernmental Relations and the Census, USA, House of Representatives

(2005) Auditul financiar 2005 – Standarde. Codul privind conduita etică şi profesională, Camera auditorilor din România

(2005) - Information System audit and Control Association – Overwiew and History, www.isaca.org

(2005) - IS Standards, Guidelines and Procedures for Auditing and Control Professionals, www.isaca.org

(2005) COBIT Control Objectives, editia III, www.isaca.org

(2004) Applying COSO'S „Entreprise Risk Assessement", The Institute of Internal Auditors

(2002) 2Si - Sécurité de Systmes d'information, Mehari et management de la sécurité.