Marin PRISĂCARU,
Banca Națională a Moldovei

RISCURILE TEHNOLOGIEI INFORMAȚIEI

Abstract: *Successful organizations recognize the benefits of information technology and understand and manage the associated risks. This article is about IT risks and the way they could influence the capability of an organization to achieve its objectives.*

Orice organizație are o misiune şi un set de obiective corelate la misiunea sa. Pe măsură ce importanța ***tehnologiei informației*** (TI) creşte pentru organizații, determinând modul în care îşi desfăşoară activitatea şi influențând direct succesul sau eşecul în atingerea obiectivelor stabilite, creşte şi importanța procesului de management al tehnologiei informației în cadrul organizației. Pentru multe organizații, informația şi tehnologia informației ce o susțin sunt cele mai valoroase, însă deseori şi cele mai puțin înțelese bunuri. Organizațiile de succes vor înțelege atât avantajele oferite de noile tehnologii, cât şi riscurile aferente lor. Conform COBIT, unul din cele cinci domenii de bază pentru guvernarea TI în cadrul organizației este managementul riscurilor aferente tehnologiei informației. Acest domeniu ține de conştientizarea riscurilor TI, stabilirea clară a nivelului riscului acceptabil, a responsabilităților pentru gestiunea acestor riscuri la toate nivelurile, definirea unui proces transparent de management. Primele trei elemente sunt necesare pentru a permite derularea adecvată a celui de al patrulea element – procesul de management al riscurilor TI.

Obiectivul procesului de management al riscurilor TI este gestionarea riscurilor generate de utilizarea tehnologiei informației într-o manieră eficace şi cost-eficientă. Eficacitatea procesului aici constă în diminuarea impactului riscurilor TI asupra capacității organizației de a-şi atinge obiectivele de activitate până la nivelul acceptabil stabilit. Managementul riscurilor TI este procesul continuu, în cadrul căruia acestea sunt identificate, impactul de realizare a lor – evaluat şi măsurile adecvate de control al riscurilor – implementate.

Riscul poate fi definit ca fiind combinația dintre probabilitatea de realizare a unui anumit eveniment şi consecințele sale. Riscul obişnuia să fie interpretat ca un eveniment nedorit cu efect negativ. Mai nou, însă, capătă popularitate conceptul conform căruia realizarea riscului poate oferi şi anumite oportunități. În această abordare creşte importanța evaluării riscurilor, deoarece doar în baza unui proces adecvat de evaluare a riscurilor vom putea identifica eventualele oportunități ce pot apărea pentru organizație ca rezultat al realizării unui anumit risc.

Totuşi, tendința generală este de a considera riscul un eveniment nedorit şi atunci

obiectivul procesului de management al riscurilor este de a identifica care sunt aceste evenimente, căile de prevenire a lui şi cum vom asigura revenirea la starea inițială în cazul realizării lor.

După cum menționam mai sus, riscurile TI pot afecta capacitatea organizației de a-şi atinge obiectivele de activitate. Respectiv, riscurile TI sunt riscuri la nivelul organizației. Orice organizație cu o viziune contemporană în domeniul managementului riscurilor de activitate are definit şi implementat un Sistem de Control Intern (SCI) aferent proceselor sale de activitate. *În cadrul SCI, de obicei, sunt definite riscurile generice pe care organizația le consideră în raport cu obiectivele sale de activitate. Acestea pot fi:* riscul financiar, riscul operațional, riscul reputațional, riscul strategic, riscul legal etc. Riscurile TI se pot manifesta prin generarea oricăror din riscurile generice menționate. De exemplu, căderea unui sistem aplicativ critic va afecta procesele de activitate ce utilizează sistemul respectiv, prin urmare riscul TI se va manifesta în cazul acesta prin riscul operațional la nivelul proceselor de activitate ce utilizează sistemul aplicativ. Compromiterea confidențialității informației cu privire la baza de clienți ai organizației poate genera riscuri financiare, reputaționale sau chiar legale.

La rândul său, riscurile TI pot fi generic identificate. Conform COBIT, pentru a corespunde necesităților de business, informația trebuie să satisfacă anumite criterii. Aceste criterii sunt: eficiența, eficacitatea, confidențialitatea, integritatea, disponibilitatea, credibilitatea, conformarea. Respectiv, orice implică utilizarea resurselor TI ale organizației şi poate amenința corespunderea informației oferite businessului acestor criterii, constituie un risc TI. *În funcție de criteriul ce poate fi afectat, riscurile TI generice pot fi:* riscul de ineficiență, riscul de ineficacitate, riscul de compromitere a confidențialității, riscul de compromitere a integrității, riscul de compromitere a disponibilității, riscul de compromitere a credibilității, riscul de neconformare.

Menționam că riscurile TI implică resurse TI. Conform COBIT, *resursele TI ale organizației sunt următoarele*: informația, aplicații-program, infrastructura informațională, oamenii. Riscurile generice, la rândul lor, se manifestă prin riscuri concrete, detaliate, aferente nemijlocit resurselor TI şi proceselor TI ce implică utilizarea resurselor respective. De exemplu, o eroare în cadrul unui sistem aplicativ poate duce la blocarea sistemului, în felul acesta informația necesară businessului nu va mai fi disponibilă. Astfel, este afectat criteriul disponibilității informației, iar riscul de erori la nivelul softului aplicativ constituie un risc de compromitere a disponibilității informației. Conceptual, modelul relațional discutat poate fi prezentat precum în figura 1.

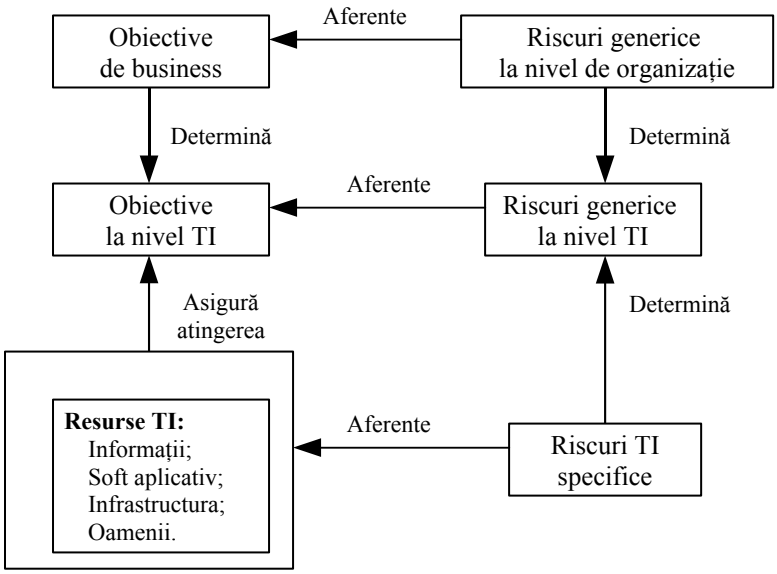

Figura 1. *Modelul relațional: obiective de business – riscuri TI*

În concluzie, orice organizație care intenționează să implementeze un Sistem de Control Intern, eficient la nivelul activității sale, nu va avea altă cale decât să conştientizeze şi să gestioneze la fel de eficiente riscurile aferent tehnologiei informației utilizate în activitatea sa. Orice altă abordare nu va fi suficient de complexă pentru a-i permite să obțină certitudine rezonabilă că riscurile aferente activității sale sunt gestionate adecvat.

Bibliografia:

1. Control Objectives for Information and Related Technologies (COBIT 4.0), Information Systems Audit and Control Association (www.isaca.org);
2. Risk Management Standard, The Institute of Risk Management (www.theirm.org);
3. Enterprise Risk Management – Integrated Framework, The Committee of Sponsoring Organization for Treadway Commission (http://www.coso.org/publications.htm).