Larisa CUJBA, UCCM

ANALIZA RISCURILOR

Abstract: *The problem of risks and methods of minimizing the risks are examined in this work. First of all we would like to view some ideas like: What does the term "the risks" mean and some ideas on this topic. Two of many standards ISO 17799 and C RAMM are examined in this work.*

Riscul este evenimentul capabil (în cazul producerii) sa exercite o influenţă asupra desfăşurării proiectului. Riscurile există în toate proiectele, dar nu neapărat se produc. Majoritatea experţilor sunt de părerea: cu cat mai degrabă va fi stabilit pericolul potenţial, cu atât mai mult timp va rămâne ca echipa de proiectanţi să-l neutralizeze sau să minimizeze pierderile. Majoritatea companiilor activitatea cărora ţine de elaborarea de proiect a produselor-program (PP), alcătuiesc propriile clasificatoare de riscuri, bazate atât pe cunoştinţele teoretice, cât şi pe experienţa de realizare a proiectelor.

În cele mai dese cazuri, complexitatea factorilor de risc este divizată convenţional în obiectivi şi subiectivi. La ***factorii obiectivi*** raportăm: modificarea datelor iniţiale condiţiilor Beneficiarului, furnizarea întârziată a utilajului, precum şi circumstanţele de forţă majoră. La rândul lor, factorii subiectivi caracterizează relaţiile reciproce dintre Beneficiar şi echipa de proiectanţi, deci tot ceea ce se referă la aşa-numitul «factor uman».

O altă variantă de clasificare a riscurilor este categorisirea lor în cele ***interne şi externe***. Aceasta modalitate este utilizată pentru definirea simplificată a pericolelor potenţiale şi a măsurilor de contracarare a acestora. Pe de o parte, sunt formate riscurile ce ţin de activitatea firmei-proiectante, iar, pe de alta parte, – riscurile la care este supus Beneficiarul. Schema prezentată se complică şi în cazul în care firma-proiectant transmite o parte din lucrări unei terţe organizaţii de subantrepriză. În această situaţie apare terţa parte şi respectivele riscuri ce nu trebuie trecute cu vederea.

Altă modalitate ar putea fi repartizarea riscurilor în două grupuri: ***evaluabile si neevaluabile***. Anume riscurile neevaluabile creează obstacole managementului de proiect. Impactul sau consecinţele riscului reprezintă influenţa riscului produs asupra posibilităţii de realizare a unor componente anumite ale planului. Impactul se referă, de regulă, la costul, graficul şi caracteristicile tehnice ale produsului elaborat. Spre exemplu, la elaborarea PP, impactul riscului poate avea ca efect necorespunderea produsului exigenţelor Beneficiarului, ba mai mult ca atât – el poate deveni de-a dreptul inutil. Impactul adeseori parcurge o perioadă

latentă – din momentul apariției riscului până la apariția modificării rezultante în sistem. Pentru evaluarea impactului riscului sunt, de regulă, utilizate unități convenționale ori scara calitativa (spre exemplu, impactul neglijabil, neesențial, esențial, mare, catastrofal). Pentru lucrul cu riscurile pozitive se impune extinderea scării în mod corespunzător.

Depistarea riscurilor proiectelor AP, poate fi convențional divizată în câteva categorii:

1. Riscurile tehnice ce țin de elaborarea noilor soluții, ori de modificarea celor vechi în legătură cu necesitatea de a spori productivitatea, ori de a obține o funcționalitate principial nouă
2. Riscurile de program ce țin de achiziționarea ori de utilizarea PP ale terțelor firme (dacă aceasta achiziție nu este supusa unui control cuvenit din partea elaboratorilor sau conducătorilor proiectului).
3. Riscurile la etapa însoțirii sistemului, inclusiv cele ce țin de amplasarea PP la Beneficiar, deservire, instruire etc.
4. Riscurile valorice ce țin de sporirea cheltuielilor ori de problemele finanțării proiectului.
5. Riscurile temporale, ce țin de necesitatea de a accelera elaborarea în virtutea unor circumstanțe de ordin extern.

CRAMM (Risk Analysis and Management Method) în anul 1985, Agenția Centrală pentru Calculatoare şi Telecomunicații (CCTA) din Marea Britanie a desfăşurat cercetări în domeniul procedeelor efective de administrare a securității informaționale pentru emiterea recomandărilor de utilizare a acestor metode în organizațiile guvernamentale în cadrul cărora este efectuată procesarea informației. Nici un procedeu examinat nu a fost recunoscut suficient de util. Atunci s-a procedat la elaborarea metodei CRAMM, iar în baza ei – a metodicii respective cu aceeaşi denumire (CRAMM: analiza şi controlul riscurilor), corespunzătoare cerințelor CCTA. Apoi au apărut câteva versiuni ale metodicii, orientate spre cerințele diferitelor organizații şi structuri de stat şi comerciale. Una din versiunile de profil „comercial" a fost înalt apreciată pe piața mijloacelor de protecție a informației. *Scopurile principale ale metodicii CRAMM sunt:*

- formalizarea şi automatizarea procedurilor de analiză şi administrare a riscurilor;
- optimizarea cheltuielilor pentru mijloacele de control şi protecție;
- planificarea şi administrarea complexă a riscurilor la toate etapele ciclului vital al sistemelor informaționale;
- reducerea timpului pentru elaborarea, şi însoțirea sistemului corporativ de protecție a informației;
- argumentarea eficienței măsurilor de protecție propuse şi a mijloacelor de control;
- administrarea modificărilor şi a incidentelor;

- menținerea continuității businessului;
- luarea deciziilor operative privind administrarea securității etc.

Valoarea resurselor. Metodica permite determinarea valorii resurselor. Acest pas este obligatoriu în varianta deplină a analizei riscurilor. Valoarea resurselor fizice în acest procedeu este determinată de prețul restabilirii în caz de distrugere. *Valoarea datelor si a produselor-program* este stabilită în următoarele situații:

- inaccesibilitatea resursei pe parcursul unei perioade mari de timp;
- distrugerea resursei-pierderea informației primite după ultima copiere de rezervă ori distrugerea ei completă;
- încălcarea confidențialității în cazurile accesului nesancționat al colaboratorilor titulari ori a persoanelor străine;
- examinarea modificării pentru cazurile când personalul admite mici erori (erorile introducerii), erori de program, erori premeditate;
- erorile ce țin de transmiterea informației: refuzul de transportare, netransportarea informației, transportarea pe o adresă incorectă.

Pentru evaluarea unui posibil prejudiciu, sunt propuse următoarele criterii:

- prejudicierea reputației organizației;
- încălcarea legislației în vigoare;
- prejudicierea sănătății personalului;
- prejudiciul cauzat de divulgarea datelor personale ale unor persoane aparte;
- pierderile financiare ca rezultat al divulgării informației;
- pierderile financiare în legătură cu restabilirea resurselor;
- pierderile în legătură cu imposibilitatea onorarii angajamentelor;
- dezorganizarea activității.

Această totalitate de criterii este utilizată în varianta comercială a metodei (profilul Standard). În alte versiuni totalitatea va fi alta, spre exemplu, în versiunea utilizata în cadrul instituțiilor guvernamentale sunt adăugați parametrii ce reflecta asemenea domenii ca securitatea națională şi relațiile internaționale. Deosebit de utilă este aplicarea mijloacelor instrumentale de tipul metodei CRAMM la efectuarea analizei riscurilor sistemelor informaționale cu exigențe sporite în domeniul SI. Aceasta permite obținerea evaluări argumentate a nivelurilor existente, şi a celor admisibile ale pericolelor, vulnerabilităților, eficienței protecției.

Concluzie: În final relatăm că ambele standarde funcționează foarte bine şi sunt recunoscute pe plan internațional. Cu ajutorul acestor standarde putem minimiza cu mult riscurile posibile.

Bibliografie:

1. Рождение нового стандарта безопасности: ISO 17799 – http://www.symantec.com/region/ru/resources/ISO17799.html
2. Методики и технологии управления информационными рисками (Сергей Петренко, Сергей Симонов) – http://citforum.ru/security/articles/risk/
3. Методические основы защиты информационных активов компании (Сергей Петренко) – http://www.citforum.ru/security/articles/zahita_aktivov/
4. Управление риском в информационных системах – http://www.security.ase.md/rus/index.html