PREMISE PENTRU PREVENIREA RISCURILOR OPERAȚIONALE GENERATE DE IT

Organizarea pe procese – condiție sine-qua-non

Desfăşurarea oricărei activităţi trebuie să respecte nişte principii manageriale, generale şi specifice. Pentru ca o organizaţie să îşi gestioneze riscurile specifice, generate de managementul impropriu al tehnologiei informaţiei, se impune o organizare pe procese. În acest sens, entitatea ar trebui să îşi organizeze managementul sistemelor informatice pe procese, utilizând cele mai bune practici, plecând de la referenţialul ITIL/ISO 20.000-2, în funcţie de profilul şi apetitul la risc, de dimensiunea entităţii şi de categoria de risc.

Călin M. Rangu
Director Adjunct,
Direcţia Supraveghere Integrată ASF

Din standarde trebuie extrase în primul rând elementele care prezintă relevanţă în managementul riscurilor operaţionale şi nu din dorinţa de a respecta formal un standard. Probabil cel mai important proces care trebuie implementat într-o organizaţie, atât în domeniul IT, cât şi în general, este **procesul de management al schimbării.**

Managementul schimbării este un proces documentat în vederea asigurării controlului asupra implementării modificărilor/schimbărilor solicitate de strategia şi planurile de afaceri şi operaţionale, la nivelul organizaţiei, al personalului, al proceselor, al sistemelor şi al operării cu furnizorii externi. Entităţile implementează procesul de management al schimbării pentru asigurarea trasabilităţii, transparenţei, documentării şi evidenţei, a minimizării dependenţelor şi a reducerii erorilor, a întârzierilor şi a fraudelor.

Schimbările se implementează prin intermediul principiilor managementului proiectelor.

Probabil zona cu cel mai mare impact, pe termen lung, este **managementul ciclului de viaţă al programelor informatice.** În acest sens se implementează un proces documentat de colectare a cerinţelor de afaceri, de analizare a lor, de redactare a specificaţiilor de afaceri şi tehnice, de alocare a resurselor, de dezvoltare software a programului informatic, de testare, promovare, de suport după implementare şi de primire de noi cerinţe pentru modificarea celor iniţiale după ce acestea operează deja în producţie.

Se iau în considerare:

- Identificarea/documentarea schimbărilor;
- Proceduri de clasificare, prioritizare şi urgenţă;
- Evaluarea impactului;
- Autorizarea schimbării;
- Managementul versiunilor;
- Distribuţia de software;
- Managementul configuraţiilor;
- Scenarii de returnare la situaţia anterioară;
- Conectarea procedurală cu managementul incidentelor şi al problemelor.

Parte a procesului de management al schimbărilor sunt:

1. Managementul versiunilor,
2. Managementul testării şi asigurării calităţii programelor informatice.

Managementul versiunilor este important în vederea managementului promovărilor (punerii în funcţiune operaţională) noilor programe informatice sau versiunilor acestora în urma unor modificări. În acest sens:

- Fiecare versiune a unui program informatic va primi un cod unic;
- Problemele de nefuncţionare sunt rezolvate în faza de testare;
- Testele de acceptanţă sunt finalizate şi semnate de utilizatorii de test şi responsabilii de activitate de afaceri;
- Toate versiunile trebuie aprobate înaintea implementării.

Referitor la **managementul testării,** acesta se va efectua în baza unei proceduri scrise şi a unui scenariu formalizat de testare, prin care să se asigure că testarea răspunde cerinţelor impuse de cele mai bune practici şi de managementul securităţii.

Managementul securităţii ar trebui să susţină implementarea unor cerinţe generale, care să asigure cel puţin:

- Integritatea, confidenţialitatea, securitatea, disponibilitatea datelor;
- Respectarea conţinutului de informaţii necesare sistemului de raportare şi luare a deciziilor;
- Reconstituirea în orice moment a rapoartelor şi informaţiilor supuse verificării;
- Stocarea şi păstrarea datelor înregistrate şi jurnalizate într-un sistem de tip bază de date pentru o perioadă de timp, în conformitate cu legislaţia aplicabilă în vigoare;
- Posibilitatea de reintegrare în sistem a datelor arhivate;
- Elemente de identificare a datelor supuse prelucrării sau verificării. Pentru operaţiuni cu specific de risc operaţional major, sistemele informatice ar trebui să asigure identificarea exactă a timpului conform unei mărci temporale – la care înregistrările au fost efectuate – şi identificarea utilizatorilor sistemului la acel moment;
- Mecanisme de securitate şi control al sistemelor informatice, pentru asigurarea păstrării în siguranţă a datelor şi informaţiilor stocate, a fişierelor şi bazelor de date, inclusiv în situaţia unor evenimente de risc.

Vulnerabilităţile sistemelor tranzacţionale ar putea fi **minimizate** prin:

- Folosirea unei scheme de criptare, atât asupra datelor trimise, cât şi asupra datelor recepţionate în vedere asigurării securităţii şi integrităţii datelor procesate;
- Mecanisme care să garanteze nerepudierea tranzacţiilor. Nerepudierea poate fi asigurată utilizând tehnici de semnătură electronică (nerepudierea originii mesajelor) şi de marcare temporală (asigurarea existenţei datei la un moment de timp).
- Jurnalizarea în timp real a informaţiei, a stării, a modificărilor;
- Mecanisme de nerepudiere a integrităţii înregistrării operaţiunilor (logurilor) de sistem informatic.