## OAMENII, PROCESELE, TEHNOLOGIILE ŞI MEDIUL EXTERN INDUC VULNERABILITĂŢI

# Evaluarea internă a riscurilor operaţionale

Evaluarea internă a riscurilor operaţionale devine din ce în ce mai importantă datorită vulnerabilităţilor generate de utilizarea sistemelor informatice, dar mai ales datorită creşterii probabilităţii ca aceste vulnerabilităţi să se materializeze.
Categorii relevante de risc se identifică pe toate **cele patru paliere ale riscurilor operaţionale:** oameni, procese, sisteme/tehnologii şi mediul extern.

**Călin M. Rangu**
Director Adjunct,
Direcţia Supraveghere Integrată ASF

În categoria **riscurilor aferente oamenilor** putem identifica: nerespectarea proceselor/procedurilor, erori de introducere manuală, cunoştinţe, experienţă şi pregătire insuficientă, personal insuficient, angajaţi-cheie, lipsă de comunicare şi cooperare, neraportare, conflict de interese, automulţumire, fraudă, operaţiuni suspecte de spălarea banilor şi finanţarea actelor de terorism, nerespectarea regimului de sancţiuni internaţionale.

Riscuri aferente **proceselor** ar putea fi generate de:

**a) Riscuri de model:** lipsa proceselor organizatorice, erori de metodologie sau model, erori de evaluare, disponibilitatea rezervelor pentru acoperirea pierderilor, complexitatea modelelor, control inadecvat al proceselor, software neadecvat obiectivelor de activitate, insuficienţa guvernanţei corporative în acest domeniu;

**b) Riscuri tranzacţionale**: erori de execuţie, erori de înregistrare, managementul inadecvat al datelor şi informaţiilor, erori de matching, compensare, colateral, complexitatea produselor, riscuri de capacitate, riscuri de evaluare, riscuri de confidenţialitate, fraude;

**c) Riscuri aferente controlului operaţiunilor:** lipsa separării drepturilor şi atribuţiilor, depăşirea limitelor, riscuri de volum, riscuri de securitate, riscuri de raportare, riscuri contabile, control inadecvat al activităţilor externalizate, întreruperea furnizării serviciilor etc.

**Riscuri aferente sistemelor/tehnologiei** pot fi cele referitoare la: sisteme inadecvate de management al tehnologiei şi securităţii, lipsa metodologiilor de dezvoltare şi testare, capacitate insuficientă de procesare, întreruperi în funcţionarea sistemelor (hardware, software, stocare, telecomunicaţii), căderi de reţea, întreruperi în furnizarea serviciilor prestate de furnizorii externi, sisteme inadecvate, protecţie inadecvată împotriva malware, riscuri de compatibilitate, riscuri generate de furnizori/vânzători, erori de programare, coruperea datelor, riscuri de recuperare după dezastre, testare necorespunzătoare a recuperării în caz de dezastru, sistem inadecvat de actualizare tehnologică, sisteme învechite, servicii necorespunzătoare de suport pentru sisteme.

**Dacă ne referim la riscuri aferente mediului extern,** am putea identifica: pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni, întreruperi în furnizarea serviciilor prestate de furnizori externi, fraude şi activităţi criminale externe, expuneri externe ale securităţii sistemelor, atacuri teroriste clasice sau informatice, criminalitate economică şi/sau informatică, căderi ale alimentării cu electricitate.

Astfel, trebuie să identificăm **sursele şi cauzele** eventualelor riscuri cheie care pot fi:

a) modificări în produsele, serviciile, personalul şi procesele existente;

b) dezvoltări de noi produse şi procese;

c) noi activităţi sau servicii;

d) afectarea activităţii de potenţiale catastrofe sau atacuri externe.

Evaluarea de risc identifică şi evaluează **natura riscului** operaţional plecând de la:

a) categoriile de risc;

b) conectivităţi şi interdependenţe;

c) modificări în modelul de lucru, precum introducerea unui nou sistem informatic, complexitatea produselor, proceselor sau tehnologiilor şi autosatisfacţie, respectiv management ineficient;

d) frecvenţa şi severitatea riscului;

e) riscul operaţional după acţiunile de diminuare a riscurilor.

În general, riscurile se **colectează** pe o structură de şablon, pe baza unor criterii standard şi se evaluează luând în considerare riscurile inerente (înaintea aplicării controalelor) şi riscurile reziduale (după ce controalele au fost aplicate).

**Măsurarea** acestor riscuri se face plecând de la rezultatele scenariilor testelor de stres, acolo unde este cazul, evaluând frecvenţa apariţiei riscurilor şi severitatea eventualelor pierderi în cadrul registrului riscurilor.

**Evaluarea frecvenţei** apariţiei riscurilor se bazează pe rapoartele interne şi externe, precum: rapoarte de audit, solicitări ale autorităţii, deviaţii faţă planul de afaceri, planuri operaţionale, bugete, opinii ale experţilor şi cele mai bune practici.

**Evaluarea severităţii** pierderilor potenţiale se poate stabili pe baza interviurilor cu angajaţi-cheie, ex ante şi ex post, variaţiile bugetelor, sesizările externe, istoria pierderilor.

Evaluarea de risc va ţine cont de **probabilitatea** ca riscul să apară în următoarele 12 luni sau altă perioadă stabilită şi de impactul, respectiv consecinţele asupra îndeplinirii strategiei şi obiectivelor de afaceri.

În cazul unei expuneri la risc mai mare decât apetitul pentru oricare riscuri se elaborează **strategii şi planuri de acţiune pentru reducerea riscurilor** şi implementarea de controale suplimentare.