Exemplu de metodologie privind evaluarea internă a riscurilor operaționale generate de sistemele informatice

Managementul riscurilor

Conceptul de management al riscului

Managementul riscului este un proces sistematic si iterativ pentru optimizarea resurselor in concordață cu politica organizațională de management a riscurilor. Managementul riscului este integrat în activitățile zilnice prin roluri și responsabilități definite în toate domeniile de activitate.
Managementul riscului ajută la includerea aspectelor de tratare a riscului în practicile de management și la luarea deciziilor pe parcursul întregului ciclu de viață al activităților. Managementul riscului poate să contribuie la maximizarea rezultatelor globale, dacă este desfășurat într-o manieră integrată, în domenii precum:

- achizitia, testarea, operarea, mentenanța și casarea sistemelor informatice, împreună cu interfețele acestora;
- controlarea consecințelor riscurilor operaționale generate de sistemele informatice;
- managementul, costurile și planificarea activităților referitoare la sistemele informatice.

Acest proces adaugă valoare datelor produse, menținute și raportate în mod regulat, iar pentru a asigura documentarea acestui proces, în evaluarea internă a riscurilor se constituie un Registru al riscurilor operaţionale generate de utilizarea sistemelor informatice de către oameni, procese, sisteme şi mediul extern. Acest registru poate fi integrat în înregistrul general al riscurilor operaționale ale entității.

Procesul de management al riscului

In cadrul procesului de management al riscului, este analizat și evaluat tot spectrul de riscuri. Evenimentele nedorite trebuie să fie analizate și evaluate din punctul de vedere al severității (impactului) și al probabilității de apariție. Măsurile de diminuare a riscurilor vor fi analizate și evaluate din perspectiva eficacității acestora, iar rezultatele măsurătorilor performanțelor și a tendinței riscurilor vor fi utilizate pentru optimizarea resurselor alocate, pentru gestionarea adecvată a riscurilor și pentru menținerea acestora în limitele de toleranță asumate de conducerea organizației.
În cadrul procesului de management al riscurilor, informațiile referitoare la riscurile potențiale sunt documentate și structurate, facilitându-se astfel luarea deciziilor pentru tratarea corespunzătoare a acestora.

Rezultatul analizei și evaluarii riscurilor inerente, precum si ale riscurilor reziduale vor fi comunicate către conducătorii organizației.

Identificarea, analiza si evaluarea riscurilor trebuie revizuită periodic sau atunci când situația o impune: la modificarea modelului de business al organizație, la orice ajustare a structurii organizatorice și a activităților ori a procedurilor de lucru în cadrul organizației, la schimbarea

tehnologiilor de procesare a informației, la modificări majore ale sistemului, în urma apariţiilor unor incidente, în urma aplicării unor controale de risc etc.

Implementarea managementului riscului

Managementul riscului necesită implicarea tuturor factorilor atât a celor cu responsabilități decizionale, cât și a celor cu atribuții executive din cadrul organizatiei şi stabilirea de linii clare de responsabilitate la nivelul tuturor structurilor organizatorice şi decizionale. Managementul riscului este un proces continuu, iterativ care constituie o parte integrantă a activității curente din cadrul organizației.

Fiecare linie de business din cadrul unei organizații își va evalua toate categoriile de risc relevante, înregistrându-le în registrul riscurilor. Se vor identifica toate potențialele probleme operaționale în patru categorii: oameni, procese, sisteme/tehnologii şi mediul extern, incluzând externalizările și furnizorii externi de produse și servicii informatice și de comunicații.

Registrul riscurilor operationale este structurat pe patru categorii:

1. Oameni
2. Procese
3. Sisteme/tehnologie
4. Extern

Riscuri aferente **oamenilor** pot fi, fără a se limita la:

- nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru;
- erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice;
- cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice;
- personal insuficient;
- dependența de angajați cheie;
- lipsă de comunicare și cooperare între angajați;
- neraportarea erorilor sau greșelilor aferente sistemelor informatice;
- alterarea datelor;
- modificarea informațiilor sau a datelor din rapoarte, fără documentarea adecvată;
- conflict de interese între personalul care dezvoltă şi cel care administrează sistemele informatice ori între utilizatorii acestora;
- lipsa unei delimitări clare între rolurile persoanelor care accesează/administrează/ dezvoltă sistemele informatice;
- automulțumire;
- fraudă;
- operațiuni suspecte de spălarea banilor și finanțarea actelor de terorism;
- nerespectarea regimului de sancțiuni internaționale.

Riscuri aferente **proceselor** pot fi, fără a se limita la:

a) ***Riscuri de model:*** lipsa proceselor organizatorice (cel puţin referitoare la managementul schimbării, al incidentelor, al problemelor, al nivelurilor de servicii, al versionărilor, al capacităţii, al disponibilităţii și al proiectelor), erori de metodologie

sau de model, erori de evaluare, disponibilitatea rezervelor pentru acoperirea pierderilor, complexitatea modelelor, control inadecvat al proceselor, software neadecvate 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 de înregistrări contabile neadecvate, control inadecvat al activităţilor externalizate, întreruperea furnizării serviciilor, neidentificarea operaţiunilor în speţă în funcţie de indicatorii de risc şi variabile analitice prestabilite.

Riscuri aferente **sistemelor/tehnologiei** pot fi, fără a se limita la:

- sistem inadecvat de management al tehnologiei şi securităţii;
- lipsa metodologiilor de dezvoltare si testare;
- capacitate insuficientă de procesare;
- întreruperi în funcţionarea sistemelor (hardware, software, stocare, telecomunicaţii);
- căderi de reţea;
- întreruperii 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.

Riscuri aferente **mediului extern** pot fi, fără a se limita la:

- pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni ori factori din afara organizaţiei;
- 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 alimentarii cu electricitate.

Structura organizației, sistemele informatice ale organizației și gestionarea riscurilor operaționale generate de acestea

Domeniul prezentei analize de impact este reprezentat de urmatoarele:

Structura organizatorică
Entitatea care face obiectul prezentului exemplu de metodologie de evaluare a riscurilor operaționale are următoarele caracteristici:

Structura organizatorică

Structura organizatorică a entității este formată din următoarele compartimente (structuri organizatorice funcționale):

1. ORGANUL SUPERIOR DE CONDUCERE: în funcție de tipul entității acesta poate să fie consiliul de administrație sau consiliu de supraveghere;
2. CONDUCEREA EXECUTIVĂ: acesta poate să fie constituit din comitet director, directori executivi, director general sau altă formă prin care se asigură conducerea activităților curente ale entității și care duce la îndeplinire hotărârile organului superior de conducere;
3. Compartiment RELAȚIA CU CLIENȚII (front office, vânzări, investitori, asigurați, participanți, membri etc): desfășoară activitățile legate de relația cu persoanele externe ale entității în vederea îndeplinirii obiectului principal de activitate (prestarea serviciilor financiare autorizate, reglementate și supravegheate de ASF);
4. Compartiment OPERAȚIUNI: desfășoară toate activitățile curente care țin de activitatea de bază a entității. Această structură organizatorică acoperă toate funcțiile operaționale ale entității;
5. Compartiment FINANCIAR-CONTABILITATE: desfășoară activitățile referitoare la operațiunile financiar-contabile și de raportare aferente înregistrărilor contabile;
6. Compartimente FUNCȚII CHEIE ALE ENTITĂȚII: În această secțiune sunt menționate mai multe structuri organizatorice distincte care asigură următoarele funcții cheie, după caz: audit intern, control intern, conformitate, managementul riscurilor, funcția actuarială, etc;
7. Compartiment TEHNOLOGIA INFORMAȚIEI: desfășoară activități specifice pentru administrarea și dezvoltarea sistemelor informatice (software, hardware și comunicații), inclusiv a paginilor de internet ale organizației;
8. Compartimente SUPORT: derulează activități de marketing, juridic, resurse umane, cercetare-dezvoltare, analiză și altele asemenea

Arhitectura infrastructurii IT:

În descrierea activitatii organizației, referitor la sistemele informatice, s-a ținut cont de următoarele aspecte:
- *arhitectura IT (doi provideri, IDP/IPS, antivirus, firewall, servere, etc)*

- *de faptul că există un BCP (business continuity plan) care cuprinde:*

- identificarea aplicațiilor critice a căror replicare este necesară în cadrul centrului de recuperare;

- descrierea infrastructurii IT din cadrul organizației;
- descrierea sistemului de disaster recovery implementat;
- descrierea personalului disponibil în cadrul organizației;
- analiza de riscuri și impactul acestora;
- definirea liniilor directoare pentru incheierea Service Level Agreements (SLA), în vederea asigurarii QoS (Quality of Service) atât cu furnizorii de echipamente, cât și cu furnizorii de sisteme de comunicații;
- descrierea modului de monitorizare a sistemului de disaster recovery în operarea curentă;
- definirea evenimentelor critice de tip dezastru;
- definirea activităților, a pașilor și a procedurilor ce compun planul BCP (Business Continuity Plan).

- *existența unei locatii alternative de procesare a datelor*

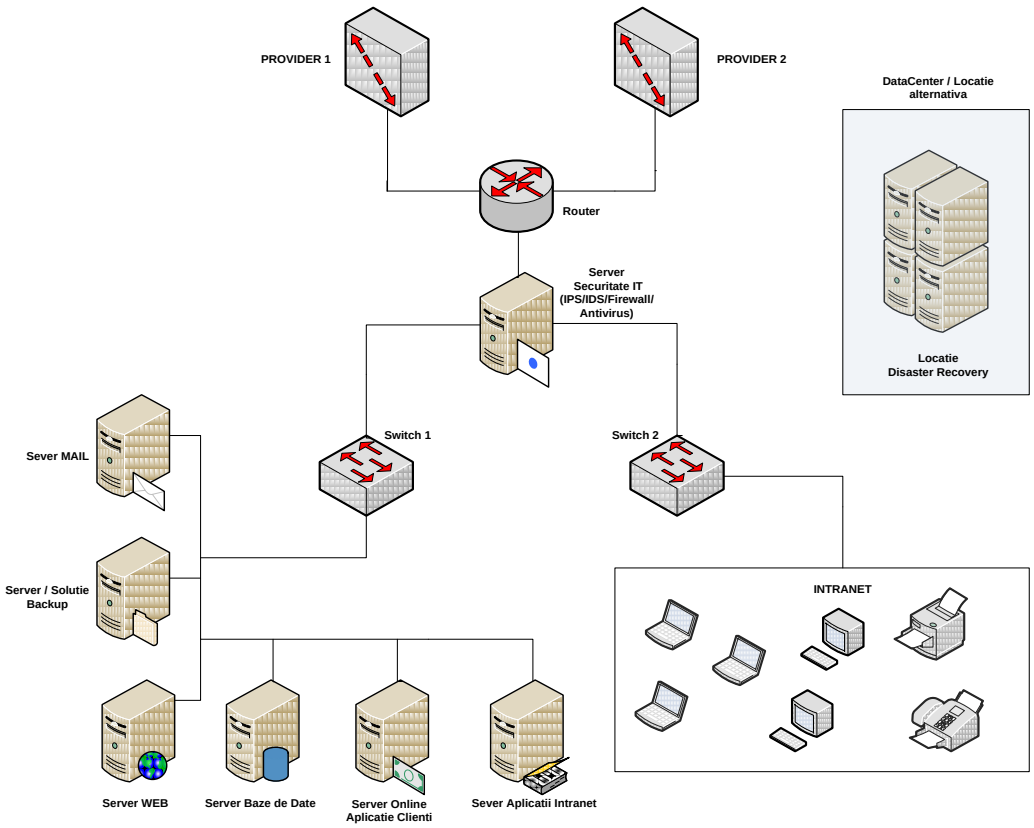
- *efectuarea back-up-urilor conform unor proceduri existente*

- *existența unei politici de securitate informatică cu următoarele obiective:*

- **Managementul securităţii informaţiei**: Măsurile managementului securităţii informaţiei vor fi implementate şi puse în aplicare în concordanţă cu obiectivele securităţii informaţiei, declaraţiile, politicile, standardele şi procedurile stabilite de conducerea organizației.
- **Clasificarea informaţiei, sistemelor şi resurselor**: Informaţiile, sistemele şi resursele vor fi clasificate corespunzător nivelului şi tipului de protecţie cerut.
- **Identificarea şi autentificarea**: toate informaţiile şi sistemele cu care institutia pune în vigoare propria identificare şi autentificare a angajaţilor, a altor utilizatori, terţelor părţi şi sistemelor.
- **Confidenţialitatea**: confidenţialitatea tuturor datelor, informaţiilor, sistemelor, documentelor şi software-urilor care este pusă în aplicare.
- **Integritatea**: integritatea datelor, informaţiilor, sistemelor, documentelor şi software-urilor care este pusă în aplicare, în funcţie de cât de critică este resursa pentru activitatea organizației.
- **Contabilizarea**: Contabilizarea şi responsabilitatea acţiunilor utilizatorilor trebuie să fie clar definite şi puse în aplicare permanent.
- **Disponibilitatea**: Toate informaţiile şi sistemele trebuie să fie disponibile utilizatorilor autorizaţi, atunci când este nevoie. , Sunt considerate oportune, în totalitate şi exacte cu recuperarea oricăror date, informaţii, software sau sisteme pierdute datorită unor evenimente nedorite şi neaşteptate (ex.întreruperea sistemului în caz de dezastru).
- **Non-repudierea**: Este un concept pentru asigurarea că o parte vătămată într-o dispută nu poate fi respinsă, sau contestată de o declaraţie de valabilitate. Sistemele trebuie să asigure că o tranzacţie informatică nu poate fi ulterior respinsă (rejectată) de acea parte vătămată.

- **Controlul accesului fizic şi logic**: Toate informaţiile şi sistemele vor fi asigurate corespunzător şi riguros cu controale de acces fizic şi logic.
- **Evaluarea riscului**: Evaluarea ameninţărilor, impactului şi vulnerabilităţilor informaţiilor a utilităţilor de procesare a informaţiilor şi a probabilităţii producerii acestora.
- **Managementul riscului**: Procesul de identificare, revizuire şi reducere sau eliminare a riscurilor de securitate, care pot afecta sistemele informatice la un cost acceptabil.
- **Instruirea şi conştientizarea privind securitatea informaţiei**: Toţi angajaţii vor fi supuşi unor programe de instruire şi conştientizare privind securitatea informaţiei.
- **Rolurile şi responsabilităţile**: Rolurile, responsabilităţile şi competenţele decizionale pentru toate părţile care au acces la resursele informatice sunt clar definite şi comunicate.
- **Conformitatea** : Personalul precum şi alţi utilizatori trebuie să fie familiarizaţi şi să se conformeze cu procedurile şi politicile băncii privind securitatea informaţiei.
- **Monitorizarea securităţii informaţiei şi raportarea**: Monitorizarea şi raportarea măsurilor de securitate a informaţiei vor fi stabilite să detecteze şi să raporteze breşele actuale şi suspecte şi vor asigura acţiuni de remediere ale acestora.

Prezentarea schematică a arhitecturii sistemelor informatice se regăseşte în figura de mai jos:



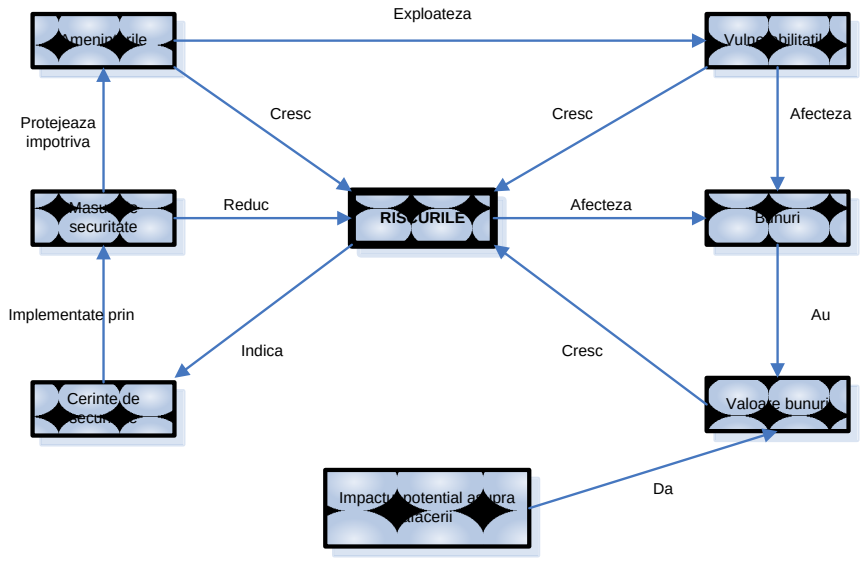
Analiza și Tratarea Riscurilor. Impactul Acestora

Organizatia a definit o abordare sistematica a evaluarii riscului in procedura internă pentru Evaluarea riscului. Metoda utilizata tine cont de cerințele legale, reglementări și de securitatea informațiilor activității organizației, precum și cele mai bune practici în domeniu. S-au determinat riscurile (pe toate cele patru categorii), criteriile de acceptare a riscurilor si s-au identificat nivelurile de risc acceptabile (apetitul și toleranța la risc).

Pentru abordarea sistematică a evaluării riscurilor sunt îndeplinite următoarele:

- S-au identificat operațiunile și activitățile organizației;
- S-au identificat sistemele informatice pe care se bazează operațiunile și activitățile identificate anterior;
- S-au identificat riscurile operaționale generate de sistemele informatice;
- S-au identificat factorii de risc (amenințările) la care care facilitează expunerea la riscurile operaționale.
- S-au identificat vulnerabilitatile care ar putea fi exploatate de aceste amenințări.
- S-a stabilit impactul și daunele asupra organizației în cazul pierderii confidentialității, integrității și disponibilității sistemelor informatice.
- S-a evaluat probabilitatea reală ca aceste evenimente să se producă.

Au fost evaluate nivelurile riscului inerent si s-a determinat dacă riscul este acceptabil sau necesită tratare. În schema de mai jos find prezentată relaționarea dintre elementele utilizate la evaluarea internă a riscurilor operaționale.



Fiecare responsabil de proces (coordonator de unitate funcțională) a identificat resursele de valoare și activitățile din cadrul structurii organizatorice (birou, serviciu, compartiment, departament, direcție etc) care sunt expuse la riscuri operaționale generate de sistemele informatice.

Resursele de valoare sunt grupate conform urmatoarelor categorii (de ex :):

- **Informatii in format electronic** (baze de date, fisiere de date, liste clienți - investitori, participanți, asigurați etc-, structuri ale bazelor de date, mesaje e-mail, fișiere cu preturi etc.);

- **Documente tipărite** (manuale de utilizare, manual și suport pentru instruiri, ghiduri, licențe, contracte furnizori / clienți, comunicări, facturi, rezultate financiare, înregistrări referitoare la personalul angajat – adrese, atestari etc.);
- **Software** (sistemul de operare, aplicatii, utilitare etc)
- **Bunuri fizice** (calculatoare, servere, echipamente de comunicare și securitate, suport media magnetic, etc);
- **Persoane** (angajați, clienți, furnizori etc.);
- **Servicii** (disponibilitate servicii de retea, telecomunicatii, încălzire, iluminat, alimentare cu apă, alarmare, servicii de stingerea incendiilor, etc.);
- **Imagine și reputatie** (mijloacele de livrare a produselor sau prestare a serviciilor, certificari existente, paginile de internet ale organizației etc.).

Stabilirea valorii resurselor și a operațiunilor

Pentru stabilirea valorii resurselor și a operațiunilor, s-au luat in considerare, numai resursele informatice și operațiunile care presupun interacțiunea cu aceste resurse. S-a definit valoarea resurselor/operațiunilor utilizand următoarea scară de valori în funcție de impactul asupra organizației:

1 – puțin importantă;
2 – necesară;
3 – vitală;

Pentru stabilirea valorilor se analizează importanța, gradul de dependență față de resursă/operațiune și pericolul pe care îl reprezintă pentru procesele organizației, asupra organizației in general și asupra clienților acesteia, atunci cand informația sau resursa își pierde integritatea, confidențialitatea și disponibilitatea.

Identificarea factorilor de risc

Pentru identificarea factorilor de risc se întocmește o listă a tuturor amenințărilor aplicabile, iar pentru fiecare amenințare se identifică vulnerabilitatile existente.

Pentru calcularea riscului se definesc, în continuare:

- **Probabilitatea riscului** (probalilitatea exploatării vulnerabilității),

Probabilitatea de a se manifesta în conditiile date este evaluată astfel:

Grad	1	2	3
Probabilitate	Neglijabilă	Slabă	Mare
Descriere	Practic nu poate apare în condiții obișnuite. Istoric nu au fost semnalate situații.	Poate apare în conditii obisnuite, dar frecvența apariției este rară.	Este probabil să se producă. Acest risc este rezonabil sa se producă în perioada imediat următoare.

- **Nivelul vulnerabilitatii** (poate să apară un incident pentru ca vulnerabilitatea să fie mai greu sau mai ușor exploatată).

Criteriile pentru evaluarea **vulnerabilitatii** sunt:

Grad	**1**	**2**	**3**
Criterii	Neglijabilă	Medie	Mare
Descriere	Există protecții sigure, testate și verificate, condițiile existente conduc la concluzia că, practic, nu poate fi exploatată aceasta vulnerabilitate.	Vulnerabilitatea poate fi exploatată, există protecții implementate, dar acestea nu au fost testate și verificate pentru toate cazurile.	Usor de exploatat, protecția este foarte slabă, ineficace în multe situații sau tehnic uzată moral.

Pentru evaluarea riscurilor şi a nivelurilor asociate pentru fiecare eveniment nedorit care poate avea impact asupra activităților desfășurate de organizație, sistemelor informatice sau a informaţiilor se realizează matricea nivelului de risc.

Nivelul riscului este o funcţie de probabilitatea de producere a unui eveniment nedorit şi de nivelul vulnerabilității asupra activităților, informațiilor sau sistemelor informatice ale organizației.

Pentru exemplificare, a fost realizată o matrice 3x3 corespunzătoare următoarelor niveluri de risc:

1. Risc mic;
2. Risc mediu;
3. Risc mare.

Exemplu matrice niveluri de risc

VULNERABILITATE				
	MARE	**Risc Mediu**	**Risc Mare**	**Risc Mare**
	MEDIE	**Risc Mic**	**Risc Mediu**	**Risc Mare**
	NEGLIJABILÃ	**Risc Mic**	**Risc Mic**	**Risc Mediu**
		NEGLIJABILÃ	**SLABÃ**	**MARE**
		PROBABILITATE		

În cazul în care organizația utilizează o altă matrice de risc prin folosirea mai multor niveluri de vulnerabilități și probabilități (4x4 sau 5x5) și a mai multor niveluri de risc (4 sau 5), se va menține practica curentă.

Activităţi necesare identificării şi evaluării riscurilor şi a măsurilor de securitate

Conducătorii structurilor organizatorice şi întreg personalul ce le compun au obligaţia de a identifica, evalua și raporta riscurile operaționale generate de sistemele informatice. Aplicarea cadrului pentru gestionarea riscurilor generate de sistemele informatice într-o organizație presupune parcurgerea următoarelor etape:

1. analiza preliminară a riscului;
2. identificarea și evaluarea riscurilor;
3. revizuirea și raportarea situației riscurilor;
4. stabilirea limitelor de toleranță;
5. implementarea și monitorizarea măsurilor de control al riscurilor.

Analiza preliminară

Persoana care identifică un risc analizează preliminar riscul identificat, procedând, pentru documentarea procesului de evaluare, la completarea unui formular de „Alertă la risc ” - stabilit de fiecare organizație și prezentat ca exemplu la finalul acestei secțiuni – cu respectarea următoarelor etape:

1 descrierea nartativă a riscului, cu respectarea următoarelor reguli:
- riscul este o situaţie, eveniment, care poate să apară. Riscul este o incertitudine şi nu ceva sigur;
- nu se identifică riscuri care nu afectează organizația;
- problemele dificile identificate nu trebuie ignorate. Ele pot deveni riscuri în situaţii repetitive din cadrul aceleiaşi structuri organizatorice sau pentru alte structuri organizatorice în care astfel de riscuri nu s-au materializat;
- riscurile nu trebuie definite numai prin impactul lor asupra activităților organizației. Impactul nu este risc, ci consecinţa exploatării unei vulnerabilități;
- riscurile nu se descriu prin negarea unei situații;
- problemele care vor apărea cu siguranţă, nu constituie riscuri, ci certitudini;
- problemele a căror apariţie este imposibilă, nu constituie riscuri, ci ficţiuni.

2 prezentarea preliminară a cauzelor, descrierea circumstanţelor şi a factorilor care favorizează apariţia riscului;

3 analizarea preliminară a consecinţelor asupra activităților și operațiunilor, în cazul materializării riscului.

4 evaluarea preliminara a expunerii la risc se realizează prin:
   a) stabilirea valorii resursei/operațiunii, pe o scală în trei trepte, ca fiind: puțin importantă (valoare=1), necesară (valoare=2) sau vitală (valoare=3).
   b) estimarea probabilității de apariţie a riscului, pe o scală în trei trepte, ca fiind: neglijabilă (valoare=1), medie (valoare=2) sau mare (valoare=3).
   c) estimarea vulnerabilității sistemului informatic, pe o scală în trei trepte, ca fiind: neglijabilă (valoare=1), medie (valoare=2) sau mare (valoare=3).
   d) evaluarea preliminară a nivelului riscului, conform matricei de risc, pe o scală cu trei trepte, ca fiind: scăzut, mediu sau mare.

e) evaluarea preliminară a valorii riscului se realizează prin adunarea valorii resursei, cu valoarea probabilității și cu cea a vulnerabilității. Valoarea maximă a riscului este 9 (3+3+3 = 9 – resursa este vitală, probabilitatea este mare și vulnerabilitatea este mare).

Notă: Explicaţiile asociate denumirii fiecărei trepte a scalelor de măsurare a valorii resurselor, a probabilităţii de apariţie şi a vulnerabilităţii pentru evaluarea riscului inerent au fost prezentate mai sus.

5 formularea unei opinii cu privire la măsurile de tratare (controalele de risc) ce ar trebuie întreprinse pentru a gestiona riscul în mod adecvat, astfel încât să se încadreze în limitele de toleranță;

6 formularul "Alertă la risc" completat corespunzător este trimis coordonatorului stucturii organizatorice.

Formular alertă la risc

<table>
<tr><td colspan="3">ORGANIZAȚIA ----------</td></tr>
<tr><td colspan="3">Structura organizatorică: ----------</td></tr>
<tr><td colspan="3">DETALII PRIVIND RISCUL</td></tr>
<tr><td rowspan="4">Descrierea riscului</td><td colspan="2">Categorie resursă IT: ----------</td></tr>
<tr><td colspan="2">Denumire resursă IT: ----------</td></tr>
<tr><td colspan="2">Amenințări (factori de risc):
1.----------
2. ----------
3. ----------
4. ----------
5. ----------</td></tr>
<tr><td colspan="2">Vulnerabilitate (descrierea riscului): ----------
----------</td></tr>
<tr><td>Evaluare valorii resursei</td><td colspan="2"><table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neimportantă; 2. necesară; 3. vitală.</td></tr>
<tr><td rowspan="2">Evaluarea riscului</td><td colspan="2">Evaluarea probabilității de apariție
<table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neglijabilă; 2. medie; 3. mare.</td></tr>
<tr><td colspan="2">Evaluarea vulnerabilității (impactului)
<table><tr><td></td><td></td><td></td></tr><tr><td>1</td><td>2</td><td>3</td></tr></table>1. neglijabilă; 2. medie; 3. mare.</td></tr>
<tr><td rowspan="2">Opinie cu privire la tipul de răspuns la risc</td><td colspan="2">Tipul de răspuns la risc (strategia adoptată): ---------
----------</td></tr>
<tr><td colspan="2">Măsuri de control le riscului recomandate:----------
----------</td></tr>
<tr><td colspan="3">Documentația utilizată pentru fundamentarea riscului identificat (dacă este cazul):----------
----------</td></tr>
<tr><td>Nume:
----------</td><td>Semnătura:
----------</td><td>Data întocmirii:
zz/ll/aaaa</td></tr>
</table>

Identificarea și evaluarea riscurilor

Coordonatorul structurii organizatorice analizează fiecare formular "*Alertă la risc",* primit de la persoanele care au efectuat analiza preliminară a riscurilor, propunând:

1 clasarea formularului "*Alertă la risc"*, dacă riscul este nerelevant;

2 înregistrarea riscului ca aparţinând activității sau operațiuni care se bazează pe sistemul informatic utilizat/administrat de structura organizatorică, caz în care confirmă existența riscului la nivelul structurii organizatorice, stabilește/confirmă nivelul riscului și propune cel puțin o măsură de tratare a acestuia.

După finalizarea acţiunii de analiză preliminară a riscurilor, conducătorul structurii organizatorice, centralizează rezultatele analizei datelor/informaţiilor cuprinse în formularele "Alertă la risc", la care anexează documentaţia privind riscurile nou-identificate.

În cadrul analizei „alertelor la risc" conducătorul structurii organizatorice desfăşoară următoarele acţiuni:

1 deliberează asupra tuturor riscurilor si stabileste riscurile pentru care să fie luată decizia de "reţinere pentru gestionare" în cadrul structurii organizatorice;
2 propunerea de **clasare** pentru riscurile considerate nerelevante;
3 deliberează asupra riscurilor propuse spre includere în Registrul Riscurilor şi face propuneri de completare a Registrului Riscurilor, cel puţin în următoarele situaţii:
   a) măsurile prin care se realizează un control satisfăcător al riscurilor exced competenţelor decizionale ale structurii organizatorice;
   b) resursele structurii organizatorice sunt insuficiente;
   c) se identifică riscuri externe structurii organizatorice, dar al căror impact afectează obiectivele stabilite pentru acesta.
4 efectuează, pentru fiecare risc identificat şi evaluat, o comparare a expunerii la risc cu limitele de toleranţă aprobate de conducerea organizației;
5 analizează rapoartele de audit, reţinând riscurile identificate prin acestea şi măsurile de control recomandate a fi implementate;
6 formulează propuneri pentru conducerea organizației, pentru fiecare risc identificat şi evaluat, cu privire la tipul de răspuns (strategia adoptată) considerat cel mai adecvat dintre cele de mai jos, decizia finală cu privire la acest aspect aparţinând conducătorului organizației:
   a) **acceptarea (tolerarea)** riscului, în cazul riscurilor cu expunere scăzută sau atunci când aplicarea unei strategii de răspuns la risc nu este posibilă;
   b) **monitorizarea** permanentă a riscului, în cazul riscurilor cu impact semnificativ, dar cu probabilitate mică de apariţie;
   c) **evitarea** riscului, cu precizarea că aplicarea acestei strategii este limitată în cazul activităţilor care ţin de obiectul de activitate al organizației și de deciziile conducerii acesteia;
   d) **transferarea (externalizarea)** riscului, îndeosebi în cazul riscurilor pentru care se înregistrează doar cheltuieli financiare care pot fi acoperite prin produse de asigurare;
   e) **tratarea (atenuarea)** riscului, caz în care se identifică măsurile posibile ce pot fi luate astfel încât riscurile să fie controlate satisfăcător, se

grupează în variante alternative, se alege varianta cea mai avantajoasă din perspectiva raportului cost/beneficiu.

7 Stabilește ordinea de priorităţi în tratarea riscurilor reţinute pentru gestionare, astfel încât expunerea la riscurile reziduale să se situeze în limitele de toleranţă aprobate;

8 stabilește măsurile de control ce trebuie luate în vederea reducerii nivelelui riscurilor (reducerea probabilității sau a impactului), termenele-limită până la care acestea trebuie implementate, precum şi persoanele responsabile cu implementarea lor prin elaborarea unui planul pentru implementarea măsurilor de control.

Conducerea organizației şi persoana (comitetul) desemnat de aceasta cu r*esponsabilități pentru gestionarea riscurilor, dacă există,* desfăşoară următoarele acţiuni:

1 primește formularele de "*Alertă la risc"* şi documentaţia aferentă pentru riscurile semnalate către fiecare structură organizatorică;

2 transmite persoanelor responsabile cu implementarea măsurilor de control, modificarea măsurilor sau a termenelor pentru riscurile aflate deja în faza de implementare a măsurilor de control intern;

3 iniţial intocmește şi ulterior completează, ori actualizează, după caz, Registrul Riscurilor, respectivei organizaţii cu datele/informaţiile despre riscurile care sunt sau care urmează a fi gestionate la nivelul tuturor structurilor organizatorice.

Revizuirea şi raportarea situaţiei riscurilor

Cel puţin anual sau ori de câte ori este cazul, conducătorii structurilor organizatorice asigură analizarea stadiului implementării măsurilor de control, a eficacităţii acestora, precum şi reevaluarea riscurilor din sfera lor de responsabilitate.

În cadrul procesului de revizuire, se analizează dacă:

1 riscurile persistă;
2 au apărut riscuri noi;
3 impactul şi probabilitatea riscurilor au suferit modificări, caz în se revizuiesc nivelurile riscurilor;
4 sunt necesare noi măsuri de control de risc şi termene pentru implementarea acestora;
5 se impune reprioritizarea riscurilor;

Anual, conducătorii structurilor organizatorice elaborează un raport cu privire la desfăşurarea procesului de gestionare/revizuire a riscurilor la nivelul structurii organizatorice. Raportul cuprinde o sinteză a activităţilor desfăşurate, în perioada de raportare, în cadrul procesului de gestionare a riscurilor, conţinând cel puţin următoarele aspecte:

1 activităţile derulate în perioada pentru care se întocmește raportul, în scopul tratării riscurilor identificate;

2 riscuri noi, tipul de răspuns şi măsurile de control instituite pentru acestea;

3 rezultatele reevaluării riscurilor, în cazul în care riscurile au fost reevaluate în perioada raportată;

4 menţiuni cu privire la întocmirea/actualizarea Registrului riscurilor;

5 alte aspecte/probleme considerate relevante, în legătură cu modul în care au fost gestionate riscurile la nivelul structurii organizatorice.

Raportul privind gestionarea şi revizuirea riscurilor cuprinde, distinct, două secţiuni referitoare la:

- riscurile cu un nivel al expunerii ridicat şi foarte ridicat, care ar putea afecta îndeplinirea obiectivelor specifice ale structurilor organizatorice;
- stadiul implementării planului, la data raportării.

Conducătorul structurii organizatorice transmite conducerii organizaţiei şi persoana (comitetul) desemnat de aceasta cu r*esponsabilităţi pentru gestionarea riscurilor, dacă există*, un exemplar al raportului, în vederea:

1 întocmirii şi actualizării Registrului Riscurilor la nivelul întregii organizaţii, prin agregarea datelor/informaţiilor cuprinse în Registrul riscurilor de la nivelul fiecărei structuri organizatorice;

2 întocmirii şi actualizării profilului de risc al organizaţiei, prin regruparea riscurilor identificate, evaluate şi ierarhizate în raport cu mărimea deviaţiei expunerii fiecărui risc de la toleranţa la risc;

3 întocmirii raportului privind evaluarea internă a riscurilor operaţionale generate de sistemele informatice pentru transmiterea lui către ASF, în conformitate cu prevederile art.14 alin.(1) lit. a) din Norma ASF nr. 6/2015. În cadrul raportului se cuprinde, distinct, o secţiune referitoare la riscurile cu un nivel al expunerii ridicat şi foarte ridicat, care ar putea afecta îndeplinirea activitatea organizaţiei.

În situaţia în care intervin modificări în conţinutul rapoartelor şi a registrelor de riscuri, conducătorii structurilor organizatorice asigură transmiterea, cătreconducerea organizaţiei, a rapoartelor şi/sau registrelor revizuite în termenul cel mai scurt posibil, dar nu mai târziu de 15 zile de la modificarea acestora.

Pentru etapa iniţială, termenul pentru transmiterea la ASF a raportului privind evaluarea internă a riscurilor operaţionale generate de sistemele informatice este de 30 iunie 2016.

Stabilirea limitelor de toleranţă (toleranţa la risc)

Condurătorii fiecărei structuri organizatorice analizează, cel puţin o dată pe an, limitele de toleranţă şi, dacă este cazul, propune revizuirea acestora, cel mai târziu până la sfârşitul lunii februarie pentru anul în curs.
Propunerile privind limitele de toleranţă revizuite se aprobă de conducerea organizaţiei (Consiliul de administraţie, Comitetul director sau Directorul general).

Toate riscurile trebuie controlate astfel încât expunerea la risc să se încadreze în limitele de toleranţă aprobate.

Limitele de toleranţă la risc au caracter obligatoriu pentru structurile organizatorice şi au aplicabilitate până la o nouă revizuire a acestora.

Implementarea şi monitorizarea măsurilor de control al riscurilor

Anual, până la finele lunii februarie, conducătorul fiecărei structuri organizatorice, întocmeşte *Planul pentru implementarea măsurilor de control ale riscurilor*, pentru anul în curs, ţinând cont şi de:

- deciziile conducerii organizației;
- recomandările cu privire la măsurile de control, cuprinse în rapoartele de audit (auditul intern, auditul IT Extern, auditul IT cu resurse interne certificate, evaluările funcției de management al riscurilor).

După aprobare, conducătorul structurii organizatorice transmite persoanelor responsabile cu implementarea măsurilor de control ale riscurilor, câte un exemplar al acestuia, pentru aplicare, precum și conducerii organizației pentru includerea lor în raportul privind evaluarea internă a riscurilor operaționale generate de sistemele informatice.

Responsabilii cu implementarea măsurilor de control informează semestrial şi ori de câte ori este cazul, pe conducătorul structurii organizatorice, cu privire la stadiul implementării măsurilor de control ale riscurilor, pentru analiză şi decizie.

Concluzii analiza riscuri

In urma analizei impactului riscurilor se pot trage urmatoarele concluzii:

1. ***Definirea evenimentelor critice***

Solutia si serviciile de protectie pentru gestionarea corespunzătoare a riscurilor operaționale generate de sistemele informatice vor acoperi urmatoarele evenimente:

- Riscuri aferente oamenilor:
  - nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru;
  - erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice;
  - cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice;
  - personal insuficient;
  - dependența de angajați cheie;
  - lipsă de comunicare și cooperare între angajați;
  - neraportarea erorilor sau greșelilor aferente sistemelor informatice;
  - alterarea datelor;
  - modificarea informațiilor sau a datelor din rapoarte, fără documentarea adecvată;
  - conflict de interese între personalul care dezvoltă și cel care administrează sistemele informatice ori între utilizatorii acestora;
  - lipsa unei delimitări clare între rolurile persoanelor care accesează/administrează/ dezvoltă sistemele informatice;
  - automulțumire;
  - fraudă;
  - operațiuni suspecte de spălarea banilor și finanțarea actelor de terorism;
  - nerespectarea regimului de sancțiuni internaționale.

- Riscuri aferente proceselor:
  - **Riscuri de model**: lipsa proceselor organizatorice (cel puţin referitoare la managementul schimbării, al incidentelor, al problemelor, al nivelurilor de servicii, al versionărilor, al capacităţii, al disponibilităţii şi al proiectelor), erori de metodologie sau de model, erori de evaluare, disponibilitatea rezervelor pentru acoperirea pierderilor, complexitatea modelelor, control inadecvat al proceselor, software neadecvate obiectivelor de activitate, insuficienţa guvernanţei corporative în acest domeniu;
  - **Riscuri tranzacționale**: erori de execuție, erori de înregistrare, managementul inadecvat al datelor și informațiilor, erori de matching, compensare, colateral, complexitatea produselor, riscuri de capacitate, riscuri de evaluare, riscuri de confidențialitate, fraude;
  - **Riscuri aferente controlului operațiunilor**: lipsa separării drepturilor și atribuțiilor, depășirea limitelor, riscuri de volum, riscuri de securitate, riscuri de raportare, riscuri de înregistrări contabile neadecvate, control inadecvat al activităților externalizate, întreruperea furnizării serviciilor, neidentificarea operațiunilor în speță în funcție de indicatorii de risc și variabile analitice prestabilite.
- Riscuri aferente sistemelor:
  - sistem inadecvat de management al tehnologiei și securității;
  - lipsa metodologiilor de dezvoltare si testare;
  - capacitate insuficientă de procesare;
  - întreruperi în funcționarea sistemelor (hardware, software, stocare, telecomunicații);
  - căderi de rețea;
  - întreruperii în furnizarea serviciilor prestate de furnizorii externi;
  - sisteme inadecvate;
  - protecție 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.
  - caderi echipamente IT
- Riscuri aferente mediului extern:
  - pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni ori factori din afara organizației;
  - întreruperi în furnizarea serviciilor prestate de furnizori externi;
  - fraude și activități criminale externe;
  - expuneri externe ale securității sistemelor;
  - atacuri teroriste clasice sau informatice;
  - criminalitate economică și/sau informatică;
  - căderi ale alimentarii cu electricitate.

2. ***Identificarea sistemelor informatice importante din cadrul organizatiei***
   În această secțiune vor fi evidențiate sistemele informatice importante, inclusiv principalele caracteristici și versiunea în lucru la momentul evaluării.

3. ***Disponibilitatea sistemului***
   Sistemul și serviciile de protectie pentru situatii de dezastru trebuie sa asigure reducerea riscurilor de indisponibilitate a sistemelor de productie cu o recuperare completa a functionalitatii sistemelor informatice intr-un interval orar de ordinul orelor.

4. ***Toleranta la dezastru***
   Toleranta la dezastru este asigurata prin tehnologia si serviciile cu grad inalt de disponibilitate care determina continuarea operarii aplicatiilor critice in cazul unui dezastru – in cadrul sistemelor organizatiei aceasta toleranta trebuie sa fie mare pentru garantarea continuitatii operationale.

5. ***Restaurarea serviciilor*** (RTO - *Recovery Time Objective*)
   Timpul de restaurare a serviciilor reprezinta timpul scurs intre producerea incidentului critic care a determinat inoperabilitatea site-ului principal si reluarea functionalitatii sistemului de catre site-ul de recuperare.
   In cadrul proiectului timpul estimat este de ***x ore*** in cazul comutarii totale datorat constrangerilor impuse de tehnologii, identificarea riscului si a masurilor necesare, convocarea personelor responsabile si asigurarea intregii functionalitati la nivelul centrului de recuperare.
   In cazul comutarii manuale in care este necesara si identificarea incidentului timpul estimat de recuperare este de ***yy minute***.
   In anumite circumstante, in conditiile in care comutarea se realizeaza automat si nu s-a produs un incident major, timp de recuperare poate fi redus substantial.

6. ***Pierderile de date*** (RPO - *Recovery Point Objective*)
   Pierderile de date reprezinta valoarea reala a pierderilor de date din momentul producerii incidentului pana la recuperarea acetuia, sau volumul de date care trebuie recreat pentru a se asigura integritatea datelor.
   Cantitatea de date acceptate a fi pierdute in cazul unui dezastru depind de urmatorii factori:
   - cantitatea de date modificate (mediu/maxim) pe unitatea de timp;
   - interdependenta dintre aplicatiile care compun sistemul informatic;
   - calitatea, mediul si latimea de banda a conexiunilor dintre cele doua locatii.

Exemplul de evaluare internă a riscurilor operaționale generate de sistemele informatice

În tabelul de mai jos este prezentat un exemplu de evaluare internă a riscurilor operaționale generate de sistemele informatice aplicată pentru o organizație ipotetică a cărei structură organizatorică și infrastructură IT a fost descrisă la începutul materialului.

Exemplul de evaluare internă a riscurilor operaționale generate de sistemele informatice (registrul riscurilor operaționale IT)

Categorie Resursă/ Activitate	Denumire sistem informatic	Valoare resursa / activitate	Risc (descriere / amenintare)	Vulnerabilitate (factori de risc)	Valoare probabili-tate	Valoare vulnerabi li-tate	Valoare risc	Masuri de control al riscului
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[3]+[6]+[7]	[8]
Categoria 1 - riscuri operaționale OAMENI								
Conducerea executivă								
Conducerea societatii	Stație de lucru / bază de date / sisteme informatice importante	3	nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru	Lipsa unor instrumente de control pentru situatia in care conducerea executiva nu respecta procesele si procedurile de lucru	1	3	7	Anexa 1
Conducerea societatii	Stație de lucru / bază de date / sisteme informatice importante	3	Automulțumire	Implementarea unor controale insuficiente sau ineficiente.	1	3	7	Anexa 1
Conducerea societatii	Stație de lucru / bază de date / sisteme informatice importante	3	operațiuni suspecte de spălarea banilor și finanțarea actelor de terorism	Lipsa filtrelor eficiente pentru tranzactiile suspecte.	1	3	7	Anexa 1
Conducerea societatii	Stație de lucru / bază de date / sisteme informatice importante	3	nerespectarea regimului de sancțiuni internaționale	Lipsa filtrelor eficiente pentru tranzactiile suspecte. Neaducerea la zi a noutatilor cu privire la sanctiunile internationale	1	3	7	Anexa 1
Conducerea societatii	Stație de lucru / bază de date / sisteme informatice importante	3	Frauda interna	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	7	Anexa 1
Relatia cu clientii								
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	7	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	7	Anexa 1

Operatiuni								
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Frauda interna	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru	Lipsa unor instrumente de control pentru situatia in care conducerea executiva nu respecta procesele si procedurile de lucru	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Automulțumire	Implementarea unor controale insuficiente sau ineficiente.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	operațiuni suspecte de spălarea banilor și finanțarea actelor de terorism	Lipsa filtrelor eficiente pentru tranzactiile suspecte.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	nerespectarea regimului de sancțiuni internaționale	Lipsa filtrelor eficiente pentru tranzactiile suspecte. Neaducerea la zi a noutatilor cu privire la sanctiunile internationale	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Frauda interna	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	modificarea informațiilor sau a datelor din rapoarte, fără documentarea adecvată	Raportarea eronata catre autoritatile de supraveghere	1	3	7	Anexa 1

Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Erori de evaluare	Evaluarea eronata a activelor societatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Erori de procesare	Procesarea eronata a documentelor justificative	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Erori de plata	Plata eronata a unor sume de bani	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	Procesarea eronata a unor operatiuni	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Frauda interna	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	dependența de angajați cheie	Inexistenta unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte	3	Personal insuficient		1	3	7	Anexa 1

	sisteme informatice importante							
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	lipsa unei delimitări clare între rolurile persoanelor care accesează/administrează/dezvoltă sistemele informatice	Proceduri de lucru neclare sau nepuse in aplicare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	conflict de interese între personalul care dezvoltă și cel care administrează sistemele informatice ori între utilizatorii acestora	Inexistenta unor proceduri privind gestiunea conflictelor de interesa sau nepunerea in aplicare a acesteia	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice	Buget de training insuficient. Lipsa implicarii managementului in acest aspect.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	alterarea datelor	Alterarea datelor din sistemele informatice, fara posibilitatea identificarii autorului si a informatiilor initiale	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru	Procese organizatorice, proceduri si instructiuni de lucru neimplementate sau inexistente	2	3	8	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Lipsă de comunicare și cooperare între angajați	Necomunicarea la timp a unor informatii critice de la un departament catre altul	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluarea eronata e necesarului de personal	1	3	7	Anexa 1
Financiar - contabilitate								
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme	2	modificarea informațiilor sau a datelor din rapoarte, fără documentarea adecvată	Raportarea eronata catre autoritatile de supraveghere	1	3	6	Anexa 1

	informatice importante							
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	Erori de evaluare	Evaluarea eronata a activelor societatii	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	Erori de procesare	Procesarea eronata a documentelor justificative	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	Erori de plata	Plata eronata a unor sume de bani	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	Procesarea eronata a unor operatiuni	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	Frauda interna	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	6	Anexa 1
Functii cheie ale entitatii								
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	dependența de angajați cheie	Inexistenta unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexa 1

Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Personal insuficient		1	3	7	Anexa 1
Tehnologia informatiei								
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	lipsa unei delimitări clare între rolurile persoanelor care accesează/administrează/dezvoltă sistemele informatice	Proceduri de lucru neclare sau nepuse in aplicare	1	3	6	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	conflict de interese între personalul care dezvoltă și cel care administrează sistemele informatice ori între utilizatorii acestora	Inexistenta unor proceduri privind gestiunea conflictelor de interesa sau nepunerea in aplicare a acesteia	1	3	6	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice	Buget de training insuficient. Lipsa implicarii managementului in acest aspect.	1	3	6	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	alterarea datelor	Alterarea datelor din sistemele informatice, fara posibilitatea identificarii autorului si a informatiilor initiale	1	3	6	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru	Procese organizatorice, proceduri si instructiuni de lucru neimplementate sau inexistente	2	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	Lipsă de comunicare și cooperare între angajați	Necomunicarea la timp a unor informatii critice de la un departament catre altul	1	3	6	Anexa 1
Suport								
Functii suport si activitati aferente	Stație de lucru / bază de date	1	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluarea eronata e necesarului de personal	1	3	5	Anexa 1
Categoria 2 - riscuri operaționale PROCESE								
Conducerea executivă								
Conducerea societatii	Stație de lucru / bază de date	3	lipsa proceselor organizatorice	Procese organizatorice neimplementate sau inexistente	2	3	8	Anexa 1
Conducerea societatii	Stație de lucru / bază de date	3	control inadecvat al proceselor	Controlul efectuat de personal necorespunzator. Neefectuarea controalelor conform cerintelor interne	1	3	7	Anexa 1
Conducerea societatii	Stație de lucru / bază de date	3	insuficiența guvernanței corporative	Inexistenta strategiei privind guvernanta corporativa. Mecanisme de guvernanta	1	3	7	Anexa 1

				corporativa necorespunzatoare				
Relatia cu clientii								
Personal si activitati front-office	Sistem front-office	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	7	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	7	Anexa 1
Operatiuni								
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	lipsa separării drepturilor și atribuțiilor	Tranzactionarea efectuata de catre personal necalificat sau fara atributii in domeniul respectiv	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	depășirea limitelor	Tranzactionarea eronata a unor instrumente financiare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de volum	Tranzactionarea eronata a unor instrumente financiare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de securitate	Alterarea datelor din sistemele informatice, fara posibilitatea identificarii autorului si a informatiilor initiale	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de raportare	Raportarea eronata catre autoritatile de supraveghere	1	3	7	Anexa 1

Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de înregistrări contabile neadecvate	Procesarea eronata a tranzactiilor cu instrumente financiare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	control inadecvat al activităților externalizate	Lipsa unor controale interne cu privire la activitati critice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	întreruperea furnizării serviciilor	Un sistem informatic critic nu poate fi accesat pentru o lunga perioada de timp	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	neidentificarea operațiunilor în speță în funcție de indicatorii de risc și variabile analitice prestabilite	Neidentificarea indicatorilor de risc. Parametrizarea necorespunzatoare a variabilelor analitice prestabilite.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	lipsa proceselor organizatorice	Procese organizatorice neimplementate sau inexistente	2	3	8	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	control inadecvat al proceselor	Controlul efectuat de personal necorespunzator. Neefectuarea controalelor conform cerintelor interne	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	insuficienţa guvernanţei corporative	Inexistenta strategiei privind guvernanta corporativa. Mecanisme de guvernanta corporativa necorespunzatoare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte	3	erori de execuție	Executarea eronata a unor operatiuni contabile	1	3	7	Anexa 1

	sisteme informatice importante							
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de înregistrare	Inregistrarea eronata a unor operatiuni economice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	managementul inadecvat al datelor și informațiilor	Neasigurarea caracteristicilor informatiilor (consistenta, durabilitate)	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de matching, compensare și colateral	Matching eronat datorat sistemelor informatice utilizate. Erori in cadrul procesului de compensare. Erori in cadrul procesului de adecvare a colateralului clientilor	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	complexitatea produselor	Erori cauzate de neintelegerea naturii economice de la baza unor produse financiare complexe	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de capacitate	Capacitate insuficienta a bazelor de date de a prelua informatiile. Capacitate insuficienta de personal de a gestiona volumul operatiunilor financiare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de evaluare	Evaluarea eronata a activelor societatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de confidențialitate	Divulgarea de informatii sensibile catre mediul exterior. Furt de date cu caracter personal	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	fraude	Fraude cauzate de personal financiar contabil cu acces la multiple sisteme si niveluri informatice.	1	3	7	Anexa 1

Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de metodologie sau de model	Definirea gresita a modelelor econometrice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de evaluare	Evaluarea eronata a activelor societatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	disponibilitatea rezervelor pentru acoperirea pierderilor	Rezerve insuficiente pentru acoperirea pierderilor operationale. Lichiditate insuficienta a activelor din rezerve	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	complexitatea modelelor	Erori cauzate de neintelegerea naturii economice de la baza unor produse financiare complexe	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	software neadecvate obiectivelor de activitate	Sofware fara functiile critice necesare. Software cu o viteza redusa de procesare, sau cu o capacitate insuficienta de procesare a informatiilor.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluarea eronata e necesarului de personal	1	3	7	Anexa 1
Financiar - contabilitate								
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de execuție	Executarea eronata a unor operatiuni contabile	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de înregistrare	Inregistrarea eronata a unor operatiuni economice	1	3	6	Anexa 1

Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	managementul inadecvat al datelor și informațiilor	Neasigurarea caracteristicilor informatiilor (consistenta, durabilitate)	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de matching, compensare și colateral	Matching eronat datorat sistemelor informatice utilizate. Erori in cadrul procesului de compensare. Erori in cadrul procesului de adecvare a colateralului clientilor	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	complexitatea produselor	Erori cauzate de neintelegerea naturii economice de la baza unor produse financiare complexe	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	riscuri de capacitate	Capacitate insuficienta a bazelor de date de a prelua informatiile. Capacitate insuficienta de personal de a gestiona volumul operatiunilor financiare	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	riscuri de evaluare	Evaluarea eronata a activelor societatii	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	riscuri de confidențialitate	Divulgarea de informatii sensibile catre mediul exterior. Furt de date cu caracter personal	1	3	6	Anexa 1
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	fraude	Fraude cauzate de personal financiar contabil cu acces la multiple sisteme si niveluri informatice.	1	3	6	Anexa 1
Functii cheie ale entitatii								
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de metodologie sau de model	Definirea gresita a modelelor econometrice	1	3	7	Anexa 1

Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de evaluare	Evaluarea eronata a activelor societatii	1	3	7	Anexa 1
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	disponibilitatea rezervelor pentru acoperirea pierderilor	Rezerve insuficiente pentru acoperirea pierderilor operationale. Lichiditate insuficienta a activelor din rezerve	1	3	7	Anexa 1
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	complexitatea modelelor	Erori cauzate de neintelegerea naturii economice de la baza unor produse financiare complexe	1	3	7	Anexa 1
Tehnologia informatiei								
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	software neadecvate obiectivelor de activitate	Sofware fara functiile critice necesare. Software cu o viteza redusa de procesare, sau cu o capacitate insuficienta de procesare a informatiilor.	1	3	6	Anexa 1
Suport								
Functii suport si activitati aferente	Stație de lucru / bază de date	1	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluarea eronata e necesarului de personal	1	3	5	Anexa 1
Categoria 3 - riscuri operaționale SISTEME								
Conducerea executivă								
Conducerea societatii	Stație de lucru / bază de date	2	sistem inadecvat de management al tehnologiei și securității	Sisteme care nu asigura functiile critice necesare. Inexistenta procedurilor de backup. Operabilitate redusa a sistemelor.	1	3	6	Anexa 1
Relatia cu clientii								
Personal si activitati front-office	Sistem front-office	2	sisteme inadecvate	Sisteme care nu asigura functiile critice necesare. Operabilitate redusa a sistemelor.	1	3	6	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	6	Anexa 1
Personal si activitati	Sistem front-office / Stație de lucru / bază de date / sisteme	2	Stergerea accidentala a informatiilor stocate in bazele de	cunostinte si pregătire insuficiente a personalului financiar contabil. Management	1	3	6	Anexa 1

front-office	informatice importante / Alte sisteme informatice importante		date	impropriu al drepturilor de acces in aplicatie				
Operatiuni								
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	sistem inadecvat de management al tehnologiei și securității	Sisteme care nu asigura functiile critice necesare. Inexistenta procedurilor de backup. Operabilitate redusa a sistemelor.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	sisteme inadecvate	Sisteme care nu asigura functiile critice necesare. Operabilitate redusa a sistemelor.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	coruperea datelor	Prezenta datelor invalide, sau a datelor ce nu pot fi accesate de către utilizatori	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	capacitate insuficientă de procesare	Capacitate insuficienta a bazelor de date de a prelua informatiile. Capacitate insuficienta de personal de a gestiona volumul operatiunilor financiare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	întreruperi în funcționarea sistemelor (hardware, software, stocare, telecomunicații)	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	căderi de rețea	Inexistenta sistemelor de backup corespunzatoare	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	întreruperii în furnizarea serviciilor prestate de furnizorii externi	Neraportarea incidentului către furnizor in timp util.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte	3	protecție inadecvată împotriva malware	Sisteme critice importante afectate de malware	1	3	7	Anexa 1

	sisteme informatice importante							
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de compatibilitate	Incapacitatea de a utiliza informatii sau fisiere necompatibile cu noile versiuni ale programelor software	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri generate de furnizori/vânzători	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de programare	Buguri, posibile brese de securitate, procesare inceata a datelor, baze de date instabile.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	riscuri de recuperare după dezastre	Plan BCP necorespunzator sau necunoscut de catre angajati. Locatie secundara improprie.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	testare necorespunzătoare a recuperării în caz de dezastru	Locatie secundara improprie. Testarea neefectuata la timp, sau efectuata partial	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	sistem inadecvat de actualizare tehnologică	Pierderi sau coruperea informatiilor existente. Atacuri cibernetice asupra sistemelor critice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	sisteme învechite	Pierderi sau coruperea informatiilor existente. Atacuri cibernetice asupra sistemelor critice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	lipsa metodologiilor de dezvoltare si testare	Dezvoltare improprie a sistemelor informatice. Testare ce nu tine cont de specificatiile de business	1	3	7	Anexa 1

Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementarile legale respective (resurse umane, PSI, autorizari / avizari autoritati locale)	1	3	7	Anexa 1
Financiar - contabilitate								
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	coruperea datelor	Prezenta datelor invalide, sau a datelor ce nu pot fi accesate de către utilizatori	1	3	6	Anexa 1
Functii cheie ale entitatii								
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	capacitate insuficientă de procesare	Capacitate insuficienta a bazelor de date de a prelua informatiile. Capacitate insuficienta de personal de a gestiona volumul operatiunilor financiare	1	3	6	Anexa 1
Tehnologia informatiei								
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	întreruperi în funcționarea sistemelor (hardware, software, stocare, telecomunicații)	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	căderi de rețea	Inexistenta sistemelor de backup corespunzatoare	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	întreruperii în furnizarea serviciilor prestate de furnizorii externi	Neraportarea incidentului către furnizor in timp util.	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	protecție inadecvată împotriva malware	Sisteme critice importante afectate de malware	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	riscuri de compatibilitate	Incapacitatea de a utiliza informatii sau fisiere necompatibile cu noile versiuni ale programelor software	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	riscuri generate de furnizori/vânzători	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	erori de programare	Buguri, posibile brese de securitate, procesare inceata a datelor, baze de date instabile.	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice	3	riscuri de recuperare după dezastre	Plan BCP necorespunzator sau necunoscut de catre angajati. Locatie secundara improprie.	1	3	7	Anexa 1

	importante							
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	testare necorespunzătoare a recuperării în caz de dezastru	Locatie secundara improprie. Testarea neefectuata la timp, sau efectuata partial	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	sistem inadecvat de actualizare tehnologică	Pierderi sau coruperea informatiilor existente. Atacuri cibernetice asupra sistemelor critice	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	sisteme învechite	Pierderi sau coruperea informatiilor existente. Atacuri cibernetice asupra sistemelor critice	1	3	7	Anexa 1
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	3	lipsa metodologiilor de dezvoltare si testare	Dezvoltare improprie a sistemelor informatice. Testare ce nu tine cont de specificatiile de business	1	3	7	Anexa 1
Personal si sisteme IT	Router (Model , Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	IPS / IDS (Model , Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Switch 1,2 (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Server Mail (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Server Backup (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Server Web (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Server BD (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Server Aplicatie Online Clienti	3	Administrare defectuasa Incendiu	Lipsa sistem automat de detectie si stingere a incediilor	2	3	8	Anexa 1

	(Model, Serie)		Cutremur Inundatie	Lipsa sistem supraveghere video Defectiune hardware				
Personal si sisteme IT	Sever Aplicatii Intranet (Model, Serie)	3	Administrare defectuasa Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si sisteme IT	Echipament1 locatie DR (Model, Serie)	3	N/A Echipament hostat intr-o locatie alternativa – DataCenter	Defectiune hardware	1	1	5	N/A
Personal si sisteme IT	Echipament2 locatie DR (Model, Serie)	3	N/A Echipament hostat intr-o locatie alternativa – DataCenter	Defectiune hardware	1	1	5	N/A
Personal si sisteme IT	Imprimante, scanere	3	Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	1	3	7	Anexa 1
Personal si sisteme IT	Echipament desktop	3	Incendiu Cutremur Inundatie	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	1	3	7	Anexa 1
Personal si sisteme IT	Aplicatie online clienti	3	Vulnerabilitati software Erori de programare Acces neautorizat Modificări neautorizate ale software-ului sau datelor Erori de programare	Lipsa testari periodice Neaplicarea la timp a update-urilor necesare Pregătire de specialitate necorespunză-toare a personalului.	2	3	8	Anexa 1
Personal si sisteme IT	Aplicatie contabilitate	3	Vulnerabilitati software Erori de programare Acces neautorizat Modificări neautorizate ale software-ului sau datelor Erori de operare	Lipsa testari periodice Neaplicarea la timp a update-urilor necesare	2	3	8	Anexa 1
Personal si sisteme IT	Aplicatie Intranet	3	Vulnerabilitati software Erori de programare Acces neautorizat Modificări neautorizate ale software-ului sau datelor Erori de programare	Lipsa testari periodice Neaplicarea la timp a update-urilor necesare Pregătire de specialitate necorespunză-toare a personalului.	2	2	7	Anexa 1
Personal si sisteme IT	Solutie securitate IT (antivirus, firewall, etc)	3	Vulnerabilitati software Erori de programare Acces neautorizat	Lipsa testari periodice Neaplicarea la timp a update-urilor necesare	3	3	9	Anexa 1
Personal si sisteme IT	Licente Sistem Operare 1	3	Vulnerabilitati software. Acces neautorizat	Neaplicarea la timp a update-urilor necesare	2	3	8	Anexa 1

				Configurarea necorespunzătoare a funcţiilor de securitate ale sistemelor de operare				
Personal si sisteme IT	Contracte	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Personal si sisteme IT	Corespondenta	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Personal si sisteme IT	Arhiva date	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Personal si sisteme IT	Declaratii	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Personal si sisteme IT	Dosare personal	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Personal si sisteme IT	Decizii	3	Acces neautorizat Dezvaluire informatii	Lipsa filtru software Continut trafic utilizatori	2	3	8	Anexa 1
Suport								
Functii suport si activitati aferente	Stație de lucru / bază de date	1	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementarile legale respective (resurse umane, PSI, autorizari / avizari autoritati locale)	1	3	5	Anexa 1
Categoria 4 - riscuri operaționale EXTERNE								
Conducerea executivă								
Conducerea societatii	Stație de lucru / bază de date	3	Pierderea persoanelor cheie	Inexistenta unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexa 1
Conducerea societatii	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	7	Anexa 1
Conducerea societatii	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	7	Anexa 1
Relatia cu clientii								
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunostinte si pregătire insuficiente a personalului financiar contabil	1	3	7	Anexa 1

	sisteme informatice importante							
Personal si activitati front-office	Sistem front-office / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Stergerea accidentala a informatiilor stocate in bazele de date	cunostinte si pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces in aplicatie	1	3	7	Anexa 1
Operatiuni								
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	întreruperi în furnizarea serviciilor prestate de furnizori externi	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Pierderea persoanelor cheie	Inexistenta unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	Vanzarea de produse necorespunzatoare clientilor respectivi	Functionarea defectuoasa a sistemelor de front office. Incadrarea defectuoasa in categoriile de risc pentru clientii noi.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	fraude și activități criminale externe	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni ori factori din afara organizației	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	atacuri teroriste clasice sau informatice	Lipsa sistemelor de siguranta si de back-up a sistemelor informatice critice	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice	3	criminalitate economică și/sau informatică	Lipsa sistemelor de siguranta si de back-up a sistemelor informatice critice	1	3	7	Anexa 1

	importante							
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	căderi ale alimentarii cu electricitate	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	expuneri externe ale securității sistemelor	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	1	3	7	Anexa 1
Personal si activitati operatiuni	Sistem operatiuni / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementarile legale respective (resurse umane, PSI, autorizari / avizari autoritati locale)	1	3	7	Anexa 1
Financiar - contabilitate								
Personalul si activitati financiar contabile	Sistem financiar contabil / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	2	fraude și activități criminale externe	Lipsa verificarilor eficace. Lipsa principiului celor patru ochi. Management impropriu al drepturilor de acces in aplicatie.	1	3	6	Anexa 1
Functii cheie ale entitatii								
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	pierderi datorate evenimentelor catastrofice/dezastrelor naturale sau generate de oameni ori factori din afara organizației	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	2	3	8	Anexa 1
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	atacuri teroriste clasice sau informatice	Lipsa sistemelor de siguranta si de back-up a sistemelor informatice critice	1	3	7	Anexa 1
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice importante	3	criminalitate economică și/sau informatică	Lipsa sistemelor de siguranta si de back-up a sistemelor informatice critice	1	3	7	Anexa 1
Functii cheie si activitati aferente	Sistem cheie / Stație de lucru / bază de date / sisteme informatice importante / Alte sisteme informatice	3	căderi ale alimentarii cu electricitate	Lipsa sistemelor de back-up pentru energie electrica sau a liniilor secundare de telecomunicatii	1	3	7	Anexa 1

	importante							
Tehnologia informatiei								
Personal si sisteme IT	Stație de lucru / bază de date / sisteme informatice importante	2	expuneri externe ale securității sistemelor	Lipsa sistem automat de detectie si stingere a incediilor Lipsa sistem supraveghere video Defectiune hardware	1	3	6	Anexa 1
Suport								
Functii suport si activitati aferente	Stație de lucru / bază de date	1	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementarile legale respective (resurse umane, PSI, autorizari / avizari autoritati locale)	1	3	5	Anexa 1

Tratarea riscurilor (masuri de control ale riscurilor propuse pentru reducerea riscurilor) (*exemplu*)

ANEXA 1 la registrul riscurilor

Nr. Crt	Eveniment nedorit	Amenințare	Vulnerabilitate asociatã	Prob. prod. even.	Nivel Impact	Nivel risc	Mãsuri de control al riscului
1.	Producerea unui incendiu	Incendiu	Absența unui sistem automat de detectie si stingere a incendiului.	Mica	Mare	Mediu	**Implementate** -Verificarea si intreținerea instalațiilor. -Existenta procedurilor de creare a fișierelor de back –up care vizeza frecvența, tipul de back-up, persoanele autorizate și verificarea periodicã. -Exista BCP, locatie alternativa de procesare a datelor. - Instruirea personalului autorizat al sistemului privind modul de acțiune la incendiu. **Masuri viitoare** -Existența unor mijloace automate de detectie si stingere a incendiului -Realizarea unor contracte de furnizare echipamente de calcul, birotica, in cazul producerii unor astfel de evenimente -Existenta unui spatiu alternativ de reluare a activitatii pentru personal.
2.	Producerea unui cutremur	Cutremur	Lipsa planurilor de continuare a activitatii sau a procedurilor de recuperare /refacere a informatiilor in caz de cutremur	Mica	Mare	Mediu	**Implementate** -Structura de rezistențã a clãdirii este solidã. -Pereții exteriori și despărțitori ai camerelor în care sunt instalate echipamentele sistemului sunt din materiale solide. -Existenta procedurilor de creare a fișierelor de back –up care vizeza frecvența, tipul de back-up, persoanele autorizate și verificarea periodicã. -Exista BCP, locatie alternativa de procesare a datelor. **Masuri viitoare** -Instruirea personalului autorizat al sistemului privind modul de acțiune in caz de cutremur. -Realizarea unor contracte de furnizare echipamente de calcul, birotica, in cazul producerii unor astfel de evenimente.
3.	Alimentarene corespunzãtoare cu energie electrica	Cãderi ale tensiunii de alimentare	Lipsa surselor neîntreruptibile de alimentare cu energie electrica.	Mica	Mare	Mediu	**Implementate** -Serverele de backup se afla intr-o locatie de tip data center avand disponibilitate de X% -Toate serverele sunt prevazute cu UPS **Masuri viitoare** - implementare replicare sincrona intre sediul central si datacenter -achizitionare generator electric

Nr. Crt	Eveniment nedorit	Amenințare	Vulnerabilitate asociatã	Prob. prod. even.	Nivel Impact	Nivel risc	Măsuri de control al riscului
4.	Copierea neautorizatã de date / software	Dezvaluire informatii	Acces neautorizat - Copierea neautorizatã de date / software	Mica	Mare	Mediu	**Implementate** -Existenta IDS, antivirus, Firewall. -Instruirea continua a personalului. -Backup periodic al datelor in data center conform procedurilor operationale existente **Masuri viitoare** -Utilizatorii cu drepturi de acces limitate ai sistemului trebuie să aibă o pregătire corespunzătoare privind utilizarea resurselor și serviciilor sistemului. -De asemenea trebuie resprectata politica de securitate existenta. -In zona serverelor si nu numai accesul se va face pe baza de cartela magnetica.
5.	Utilizarea necorespunzãtoare a resurselor și serviciilor sistemului (erori de utilizare)	Erori de operare ale personalului	Configurarea necorespunzãtoare a funcțiilor de securitate ale sistemelor de operare.	Mica	Mare	Mediu	**Implementate** - Exista elaborata o politica de securitate care să țină cont de rolul și misiunea sistemului, grupele de utilizatori autorizați ai sistemului și de aplicarea principiului necesității de a cunoaște. -Exista elaborarta o procedura de creare a fișierelor de back –up care să vizeze frecvența, tipul de back-up, persoanele autorizate și verificarea periodică a fișierelor de back-up. -S-a creat o locatie alternativa de backup in DataCenter-ul X - Toate update-urile pe aplicatiile software se testeaza pe mediul de test inainte de implemtarea in mediul de productie **Masuri viitoare** -Cursuri de specialitate
			Lipsa fișierelor de back-up.	Mica	Mare	Mediu	
			Pregãtire de specialitate necorespunzãtoare a personalului.	Mica	Mediu	Mic	
		Erori de programare	Configurarea necorespunzãtoare a funcțiilor de securitate ale sistemelor de operare.	Mica	Mare	Mediu	
			Lipsa fișierelor de back-up.	Mica	Mare	Mediu	
			Pregãtire de specialitate necorespunzãtoare a personalului.	Mica	Mare	Mediu	
		Modificări neautorizate ale software-ului	Lipsa fișierelor de back-up.	Mica	Mare	Mediu	
			Pregãtire de specialitate necorespunzãtoare a personalului.	Mica	Mare	Mediu	