RAPORT ANUAL / INFORMARE ANUALĂ

privind desfăşurarea procesului de management al riscurilor în anul 2024 la nivelul

MULTI-TRANS S.A.

Scopul raportului:

Analizarea riscurilor care pot influența activitatea corespunzătoare a societății

Analiza procesului de management al riscurilor pe anul 2024. În cadrul procesului de revizuire, se analizează dacă:

-riscurile persistă

-au apărut noi riscurile

-impactul şi probabilitatea riscurilor au suferit modificări, caz în care se revizuiesc nivelurile riscurilor

-sunt necesare noi măsuri de control de risc şi termenele pentru implementarea acestora

-se impune reprioritizarea riscurilor

I. Cadrul legislativ Principalele acte normative care stau la baza reglementării *Managementului riscurilor* (MR) sunt următoarele: ➢ Ordonanţa Guvernului nr. 119/1999 privind controlul intern/managerial şi controlul financiar preventiv, republicată, cu modificările şi completările ulterioare; ➢ Ordinul Secretarului General al Guvernului nr. 600/2018 privind aprobarea Codului controlului intern managerial al entităţilor publice; ➢ Ordinul Secretarului General al Guvernului nr. 201/2016 pentru aprobarea Normelor metodologice privind coordonarea, îndrumarea metodologică şi supravegherea stadiului implementării şi dezvoltării sistemului de control intern managerial la entităţile publice; ➢ Legea nr. 174/2015 pentru aprobarea Ordonanţei de urgenţă a Guvernului nr. 86/2014 privind stabilirea unor măsuri de reorganizare la nivelul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative.

1. Sinteza Registrului de riscuri aferent anului raportării

Structura organizatorică a entității este formată din următoarele compartimente, conform organigramei societății :

1. ORGANUL SUPERIOR DE CONDUCERE: consiliul de administrație

2. CONDUCEREA EXECUTIVĂ: director general, asigură conducerea activităților curente ale entității și duce la îndeplinire hotărârile organului superior de conducere

3. Compartimentul SERVICIUL TEHNIC-ADMINISTRATIV: desfășoară toate activitățile curente, care țin de aprovizionare, de atelier mecanic/service autobuze, de organizarea pazei și a curățeniei

4. Compartimentul SERVICIUL FINANCIAR-CONTABILITATE: desfășoară activitățile referitoare la operațiunile financiar-contabile și de raportare aferente înregistrărilor contabile

5. Compartimentul DEPARTAMENTUL COLOANĂ AUTO ȘI AUTOGARĂ: desfășoară activitățile de prestare a serviciului de transport.

În urma Procesului-verbal al ședinței de analiză a riscurilor, s-au dezbătut urmatoarele riscuri:

- **Din partea serviciului tehnic-administrativ:**

  - întreruperi în furnizarea serviciilor prestate de furnizori (energie electrică, combustibil)

  - aprovizionarea pieselor de schimb la autobuzele invechite inca aflate in folosinta

- **Din partea departamentului de coloană auto și autogară:** - parc auto învechit – această problemă se va rezolva odată cu schimbarea autobuzelor cu autobuze electrice. Investiția efectuată de UAT-ul este în stadiu de finalizare. Au fost predate autobuze electronice, insa mai sunt in folosiinta 10 buc. de autobuze vechi.

- **Din partea servicului financiar-contabil și juridic:**

  Digitalizarea raporturilor fiscale. Raportările în scop financiar-contabil și fiscal devin din ce în ce mai complexe și mai sofisticate. În contextul digitalizării continue și al direcției tot mai evidente înspre tehnologizare, și România a adoptat, în ultimii ani, măsuri pentru modernizarea sistemelor Agenției Naționale de Administrare Fiscală (ANAF), care vizează schimbul de informații în timp real între ANAF și contribuabili.

Registrul riscurilor operaționale este structurat pe patru categorii:

1. Oameni

2. Procese

3. Sisteme/tehnologice

4. Extern

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

- nerespectarea proceselor, procedurilor sau a instructiunilor de lucru;

- erori de introducere manuala sau de utilizare neadecvata a sistemelor informatice;

- cunostințe, experiență și pregătire insuficientă a personalului care utilizează sau deservește sistemele informatice;

-personal insuficientă;

- dependență de angajați cheie;

-lipsă de comunicare și cooperare între angajați;

- alterarea datelor;

- modificarea informațiilor sau a datelor din rapoarte, fără documentare 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 sanctiuni internaționale;

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

-*Riscuri de model:* lipsa proceselor organizatorice (cel puțin referitoare la managementul schimbării, al incidentelor, al problemelor, al nivelurilor de servicii, al capacității, al disponibiltății 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 obiectelor de activitate, insuficiența guvernanței corporative în acest domeniu.

-*Riscuri tranzacționale:* erori de execuție, erori de înregistrare, managementul inadecvat al datelor și informațiilor, erori de compensare, colateral, 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 de speță în funcție de indicatorii de risc și variabile analitice prestabilite.

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

-sistem inadecvat de manegement al tehnologiei și securității;

-lipsa metodologiilor de dezvoltare și testare;

-capacitate insuficientă de procesare;

-întreruperi în funcționarea sistemelor (hardware, software, stocare, telecomunicații);

- căderi de rețea;

-întreruperi în furnizarea serviciilor prestate de furnizorii externi;

-sisteme inadecvate;

-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 sistemele.

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

-pierderi datorate evenimentelor catastrofice/dezastre 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 su informatice

-criminalitate economică ți/sau informatică

-căderi ale alimentării cu electricitate

2. Stadiul implementării măsurilor de control

Fiecare compartiment este verificat de persoana competentă în parte, astfel este urmărită starea actuala a fiecăruia.

3. Revizuirea riscurilor

Revizuirea riscurilor este efectuat anual.

1. Riscuri reziduale

- folosirea uneltelor, sculelor în mod necorespunzător
- parcurgerea unor trasee ocolitoare cu autobuze
- solicitarea unor piese de schimb necorespunzătoare

2. Riscuri care persistă

- - o parte a parcului auto învechit (10 buc)

3. Riscuri nou-identificat – risc operațional generat de Legea nr.99 / 2016 privind achizitiile sectoriale.

4. Monitorizarea riscurilor de corupţie, după caz – nu este cazul

5. Registrul de riscuri actualizat - anual

6. Concluzii şi propuneri: Anexa 1 la Registrul riscurilor

Apreciem, că în anul 2024 , procesul de gestiune al riscurilor s-a desfăşurat la un nivel, care a permis îndeplinirea obiectivelor generale și obiectivelor specifice al activității societății.

Președintele comisiei

Contabil șef – Szórádi Edit

S.C. MULTI-TRANS S.A.
Sfântu Gheorghe
NR. ÎNREG.: 876 / 16.12.2024

PROCES-VERBAL AL ȘEDINȚEI DE ANALIZĂ A RISCURILOR

Data ședintei: 16.12.2024

Participanți: Membrii Comisiei de gestionare a riscurilor

- Szórádi Edit - contabil șef- președintele comisiei
- Roman Rozalia - asistent manager - secretar
- Antal Éva - economist - membru
- Dénes Alexandru - șef coloană - membru
- Kerekes Attila - șef birou tehnic - membru

Conform organigramei, in ședința au fost convocate:

Compartimentul SERVICIUL TEHNIC-ADMINISTRATIV: desfășoară toate activitățile curente, care țin de aprovizionare, de atelier mecanic/service autobuze, de organizarea pazei și a curățeniei
Compartimentul SERVICIUL FINANCIAR-CONTABILITATE: desfășoară activitățile referitoare la operațiunile financiar-contabile și de raportare aferente înregistrărilor contabile
Compartimentul DEPARTAMENTUL COLOANĂ AUTO ȘI AUTOGARĂ: desfășoară activitățile de prestare a serviciului de transport.

Am revenit asupra problemelor dezbătute în cadrul ședinței din data de 27.12.2023, a riscurilor prezentate de fiecare membru în parte pe compartimente, au fost analizate recomandările, propunerile privind dificultățile întâmpinate și s-a constatat că au fost realizate.

În momentul ședinței birourile sunt în clădirea principală a Parcului Industrial din Câmpul Frumos, iar atelierul, magazia centralaă și autoparcul sunt la Câmpul Frumos, atelier închiriat până la finalizarea sediului societății. Finalizarea sediului societății se estimează la începutul primului trimestru al anului 2025, moment în care atât personalul societății, cât și anexele reprezentând garajele, autoparcul, atelierul, magazia centrală – vor fi în aceeași clădire.

Cu ocazia acestei ședințe s-au prelucrat riscurile cu:

Nr.crt.	Riscul analizat / Dificultăți întâmpinate	Recomandări, propuneri
01.	Achizitii publice prin intermediul SEAP	Respectarea procedurii de achiziție publica, a Legii 99/2016
02.	Erori de programare, modificări neautorizate ale software-ului, dezvăluire informații	Utilizatorii cu drepturi de acces limitate ai sistemului trebuie să aibă o pregătire corespunzătoare privind

		utilizarea resurselor și serviciilor sistemului.
03.	Erori de programare, erori de operare ale personalului	Pregătire corespunzătoare a personalului, de specialitate. Verificarea periodică a fișierelor
04.	Întreruperi în furnizarea serviciilor prestate de furnizori externi	Raportarea incidentului către furnizor în timp util
05.	Sistem inadecvat de actualizare tehnologică	Conformarea cu reglementările legale respective
06.	Riscuri de compatibilitate	Incompabilitate cu noile versiuni ale programelor software – update-uri din timp trebuiesc făcute
07.	Sisteme învechite	Atacuri cibernetice
08.	Incendiu	Existența unor automate de detecție și stingere a incendiului.
09.	Producerea unui cutremur	Instruirea personalului autorizat al sistemului privind modul de acțiune în caz de cutremur
10.	Alimentare necorespunzătoare cu energie electrică	Achiziționare generator electric
11.	Copiere neautorizată de date / software	Utilizatorii cu drepturi de acces limitate ai sistemului trebuie să aibă o pregătire corespunzătoare privind utilizarea resurselor și serviciilor sistemului
12.	Erori de operare ale personalului / Erori de programare – utilizare necorespunzătoare a sistemului	Elaborarea unei politici de securitate care să țină cont de rolul și misiunea sistemului.
13.	Modificări neautorizate ale software-ului	Elaborarea unei proceduri de creare a fișierelor de back-up.

Sfântu Gheorghe, la 16.12.2024

S.C. Multi-Trans S.A.
Sfântu Gheorghe, str. Császár Bálint, nr. 6, jud. Covasna, România
Nr. Inreg. Reg. Com.: J/14/287/1998, C.U.I.: RO 555397, capital Social:177.567,5lei

Semnează membrii comisiei de gestionare a riscurilor:

Szórádi Edit - contabil șef- președintele comisiei .....

Roman Rozalia - asistent manager - secretar .....

Antal Éva - economist – membru .....

Dénes Alexandru - șef coloană - membru .....

Kerekes Attila - șef birou tehnic - membru .....

REGISTRUL RISCURILOR

Evaluare internă a riscurilor operaţionale

Categorie Resursă / Activitate	Denumire sistem informatic	Valoare Resursă Activitate	Risc (descriere / ameninţare)	Vulnerabilitate (factori de risc)	Valoare probabilitate	Valoare Vulnerabilitate	Valoare risc	Măsuri de control al riscului
1	2	3	4	5	6	7	3+6+7	8
Categoria 1 – riscuri operaţionale OAMENI								
Conducerea societăţii	Staţie de lucru / bază de date sisteme informatice importante	3	nerespectarea proceselor, proce-durilor sau a instrucţiunilor de lucru	Lipsa unui instrument de control pentru situaţia în care conducerea executivă nu respectă procesele şi procedurile de lucru	1	3	7	Anexa 1
Conducerea societăţii	Staţie de lucru / bază de date sisteme informatice importante	3	Automulţumire	Implementarea unor controale insuficiente sau ineficiente	1	3	7	Anexă 1
Conducerea societăţii	Staţie de lucru / bază de date sisteme informatice importante	3	operaţiuni suspecte de spălarea banilor şi finanţarea actelor de terorism	Lipsa filtrelor eficiente pentru tranzacţiile suspecte	1	3	7	Anexă 1
Conducerea societăţii	Staţie de lucru / bază de date sisteme informatice importante	3	nerespectarea regimului de sancţiuni internaţionale	Neaducerea la zi a noutăţilor cu privire la sancţiuni internaţionale	1	3	7	Anexă 1
Conducerea societăţii	Staţie de lucru / bază de date sisteme informatice importante	3	Fraudă internă	Lipsa verificărilor eficace. Lipsa principiului celor patru ochi Managementul impropriu al drepturilor de acces în aplicaţie.	1	3	7	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	modificarea informaţiilor sau a date-lor din raportare, fără documentarea adecvată	Raportarea eronată către autorităţile de supraveghere	1	3	6	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	erori de introducere manuală sau de utilozare neadecvată a sistemelor informatice	Procesare eronată a unor operaţiuni	1	3	6	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	Ştergerea accidentală a informaţiilor stocate în bazele de date	Procesare eronată a unor operaţiuni	1	3	6	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	Erori de plată	Plata eronată a unor sume de bani	1	3	6	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	Fraudă internă	Lipsa verificărilor eficace. Lipsa principiului celor patru ochi	1	3	6	Anexă 1
Personal şi activităţi operaţiuni	Sistem de operaţiuni / Staţie de Lucru / bază de date / Sisteme informatice importante	3	lipsa unei delimitări clare între rolurile persoanelor care accesează / Administrează sistemele informatice	Proceduri de lucru neclare sau nepuse în aplicare	1	3	7	Anexă 1
Personal şi activităţi operaţiuni	Sistem de operaţiuni / Staţie de Lucru / bază de date / Sisteme informatice importante	3	alterarea datelor	Alterarea datelor din sisteme infor-matice, fără posibilitatea identificării autorului şi a informaţiilor iniţiale	1	3	7	Anexă 1

Personal și activități operațiuni	Sistem de operațiuni / Stație de Lucru / bază de date / Sisteme informatice importante	3	Lipsă de comunicare și cooperare între angajați	Necomunicarea la timp a unor informații critice de la un departament la altul	1	3	7	Anexă 1
Personal și activități operațiuni	Sistem de operațiuni / Stație de Lucru / bază de date / Sisteme informatice importante	3	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluare eronată a necesarului de personal.	1	3	7	Anexă 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	lipsa unei delimitări clare între rolurile persoanelor care accesează / Administrează sistemele informatice	Proceduri de lucru neclare sau nepuse în aplicare	1	3	6	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	Conflict de interese între personalul care dezvoltă și cel care administrează sistemel informatice	Inexistența unei proceduri privind gestiunea conflictelor de interese sau nedepunerea în aplicare a acesteia	1	3	6	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	alterarea datelor	Alterarea datelor din sistemele informatice, fără posibilitatea identificării autorului și a informațiilor inițiale	1	3	6	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	Lipsă de comunicare și cooperare între angajați	Necomunicarea la timp a unor informații critice de la un departament către altul	1	3	6	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	nerespectarea proceselor, procedurilor sau a instrucțiunilor de lucru	Procese organizatorice, proceduri și instrucțiuni de lucru neimplementate sau inexistente	2	3	7	Anexa 1
Categoria 2 – riscuri operaționale PROCESE								
Conducerea societății	Stație de lucru / bază de date	3	lipsa proceselor organizatorice	Procese organizatorice neimplementate sau inexistente	2	3	8	Anexa 1
Conducerea societății	Stație de lucru / bază de date	3	control inadecvat al proceselor	Neefectuarea controalelor conform cerințelor interne	1	3	7	Anexa 1
Conducerea societății	Stație de lucru / bază de date	3	insuficiența guvernanței corporative	Inexistența strategiei privind guvernanța corporativă. Mecanisme necorespunzătoare	1	3	7	Anexa 1
Personalul și activități Fin-ctb	Sistem financiar-contabil Stație de lucru / bază de date sisteme informatice importante	2	Erori de execuție	Plata eronată a unor sume de bani	1	3	6	Anexă 1
Personalul și activități Fin-ctb	Sistem financiar-contabil Stație de lucru / bază de date sisteme informatice importante	2	Erori de înregistrare	Înregistrarea eronată a unor operațiuni economice	1	3	6	Anexă 1
Personalul și activități Fin-ctb	Sistem financiar-contabil Stație de lucru / bază de date sisteme informatice importante	2	Riscuri de capacitate	Capacitatea insuficientă a bazelor de date de a prelua informațiile. Capacitate insuficientă de personal de a gestiona volumul op-lor financiare	1	3	6	Anexă 1
Personalul și activități Fin-ctb	Sistem financiar-contabil Stație de lucru / bază de date sisteme informatice importante	2	Riscuri de confidențialitate	Divulgarea de informații sensibile către mediul exterior. Furt de date cu caracter personal.	1	3	6	Anexă 1
Personalul și activități	Sistem financiar-contabil Stație de lucru / bază de date	2	Fraude	Fraude cauzate de personal financiar contabil cu acces la multiple sisteme și niveluri informatice	1	3	6	Anexă 1

Fin-ctb	sisteme informatice importante							
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	2	software neadecvate obiectivelor de activitate	Software fără funcțiile critice necesare. Software cu o viteză redusă de procesare, sau cu o capacitate insuficientă de procesare a informațiilor	1	3	6	Anexa 1
Funcții suport și activități aferente	Stație de lucru / bază de date	1	Personal insuficient	Proceduri de recrutare ineficiente. Buget de resurse umane insuficient. Evaluarea eronată a necesarului de personal/	1	3	5	Anexa 1
Categoria 3 – riscuri operaționale SISTEME								
Conducerea societății	Stație de lucru / bază de date	2	sistem inadecvat de management al tehnologiei și securității	Sisteme care nu asigură funcțiile critice necesare. Operabilitate redusă a sistemelor.	1	3	6	Anexa 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	sistem inadecvat de management al tehnologiei și securității	Sisteme care nu asigură funcțiile critice necesare. Inexistența procedurilor de beckup. Operabilitatea redusă a sistemelor.	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	sisteme inadecvate	Sisteme care nu asigură funcțiile critice necesare. Operabilitatea redusă a sistemelor.	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	coruperea datelor	Prezența datelor invalide, sau a datelor ce nu pot fi accesate de către utilizatori	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	capacitatea insuficientă de procesare	Capacitate insuficientă a bazelor de date de a prelua informațiile. Capacitate insuficientă de personal de a gestiona volumul op-lor financiare	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / 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 electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	căderi de rețea	Inexistența sistemelor de backup corespunzătoare	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	întreruperi în furnizarea serviciilor prestate de furnizorii externi	Neraportarea incidentului către furnizor în timp util	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	riscuri de compatibilitate	Incapacitatea de a utiliza informații sau fișiere necompatibile cu noile versiuni ale programelor software	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	riscuri generate de furnizori / vânzători	Lipsa sistemelor de back-up pentru energie electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	sistem inadecvat de actualizare tehnologică	Pierderi sau coruperea informațiilor existente. Atacuri cibernetice asupra sispemelor critice	1	3	7	Anexă 1

Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementările legale respective (resurse umane, PSI, autorizări / avizări autorități locale)	1	3	7	Anexă 1
Personalul și activități Fin-ctb	Sistem financiar-contabil Stație de lucru / bază de date sisteme informatice importante	2	coruperea datelor	Prezența datelor invalide, sau a datelor ce nu pot fi accesate de către utilizatori	1	3	6	Anexă 1
Personal și 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 electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	căderi de rețea	Inexistența sistemelor de beckup corespunzătoare	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	riscuri de compatibilitate	Incapacitatea de a utiliza informații sau fișiere necompabilitatw cu noile versiuni ale programelor software	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	riscuri generate de furnizori / vânzători	Lipsa sistemelor de back-up pentru energie electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	testare necorespunzătoare a riscuri generate de furnizori / vânzători	Locație secundară improprie. Testarea neefectuată la timp, sau efectuată parțial	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	sistem inadecvat de actualizare tehnologică	Pierderi sau coruperea informațiilor existente. Atacuri cibernetice asupra sispemelor critice	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	sisteme învechite	Pierderi sau coruperea informațiilor existente. Atacuri cibernetice asupra sispemelor critice	1	3	7	Anexa 1
Personal și sisteme IT	Stație de lucru / bază de date sisteme informatice importante	3	lipsa metodologiilor de dezvoltare și testare	Dezvoltarea improprie a sistemelor informatice. electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexa 1
Personal și sisteme IT	Router, Switch, Server (Model, serie)	3	Administrare defectuoase Incendiu, cutremur Inundație	Lipsa sistem automat de detecție și stingere a incendiilor. Lipsă sistem supraveghere video. Defecțiune hardware.	2	3	8	Anexa 1
Personal și sisteme IT	Aplicație online clienți	3	Vilnerabilități software. Erori de prog-ramare. Acces neautorizat. Modificări neautorizate ale software-ului/ datelor	Lipsă testări periodice. Neaplicarea la timp a Update-urilor necesare. Pregătire de specialitate necorespunzătoare a personalului	2	3	8	Anexa 1
Personal și sisteme IT	Aplicație contabilitate	3	Vilnerabilități software. Erori de prog-ramare. Acces neautorizat. Modificări neautorizate ale software-ului/ datelor	Lipsă testări periodice. Neaplicarea la timp a Update-urilor necesare.	2	3	8	Anexa 1
Personal și			Vilnerabilități software.	Lipsă testări periodice. Neaplicarea la timp a				

sisteme IT	Soluție securitate IT (antivirus, firewall, etc.)	3	Erori de programare. Acces neautorizat.	Update-urilor necesare.	3	3	9	Anexa 1
Personal și sisteme IT	Contracte	3	Acces neautorizat Dezvăluire informații	Lipsă filtru software. Conținut trafic utilizatori	2	3	8	Anexa 1
Personal și sisteme IT	Corespondență	3	Acces neautorizat Dezvăluire informații	Lipsă filtru software. Conținut trafic utilizatori	2	3	8	Anexa 1
Personal și sisteme IT	Declarații	3	Acces neautorizat Dezvăluire informații	Lipsă filtru software. Conținut trafic utilizatori	2	3	8	Anexa 1
Personal și sisteme IT	Dosare personale	3	Acces neautorizat Dezvăluire informații	Lipsă filtru software. Conținut trafic utilizatori	2	3	8	Anexa 1
Personal și sisteme IT	Decizii	3	Acces neautorizat Dezvăluire informații	Lipsă filtru software. Conținut trafic utilizatori	2	3	8	Anexa 1
Categoria 4 – riscuri operaționale EXTERNE								
Conducerea societății	Stație de lucru / bază de date	3	Pierderea persoanelor cheie	Inexistența unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexa 1
Conducerea societății	Sistem front-office / Stație de lucru/ bază de date / sisteme informatice importante	3	erori de introducere manuală sau de utilizare neadecvată a sistemelor informatice	cunoștințe și pregătire insuficiente a personalului financiar contabil	1	3	7	Anexă 1
Conducerea societății	Sistem front-office / Stație de lucru/ bază de date / sisteme informatice importante	3	Ștergerea accidentală a informațiilor stocate în bazele de date	cunoștințe și pregătire insuficiente a personalului financiar contabil. Management impropriu al drepturilor de acces în aplicație.	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	întreruperea în furnizarea serviciilor prestate de furnizori externi	Lipsa sistemelor de back-up pentru energie electrică sau a liniilor secundare de telecomunicații	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	pierderea persoanelor cheie	Inexistența unui back-up pentru persoanele cheie din companie. Proceduri de recrutare ineficiente.	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	fraude și activități criminale externe	Lipsa verificărilor eficace. Lipsa principiului celor patru ochi. Managementul impropriu al drepturilor de acces în aplicație.	1	3	7	Anexă 1
Personalul și activități operațiuni	Sistem operațiuni / Stație de lucru / bază de date / sisteme informatice importante	3	pierderi datorate evenimentelor catastro- Fice / dezastrelor naturale sau generate de oameni din afara organizației	Lipsa sistem automat de detecție și stingere a incendiilor. Lipsă sistem supraveghere video.	2	3	8	Anexă 1
Personalul și activități	Sistem operațiuni / Stație de lucru / bază de date /	3	atacuri teroriste clasice sau informatice	Lipsa sistemelor de siguranță și de back-up a sistemelor informatice critice	1	3	7	Anexă 1

operaţiuni	sisteme informatice importante							
Personalul şi activităţi operaţiuni	Sistem operaţiuni / Staţie de lucru / bază de date / sisteme informatice importante	3	criminalitate economică şi / sau informatică	Lipsa sistemelor de siguranţă şi de back-up a sistemelor informatice critice	1	3	7	Anexă 1
Personalul şi activităţi operaţiuni	Sistem operaţiuni / Staţie de lucru / bază de date / sisteme informatice importante	3	căderi ale alimentării cu electricitate	Lipsa sistemelor de back-up pentru energie electrică sau a liniilor secundare de telecomunicaţii	1	3	7	Anexă 1
Personalul şi activităţi operaţiuni	Sistem operaţiuni / Staţie de lucru / bază de date / sisteme informatice importante	3	expuneri externe ale securităţii sistemelor	Lipsa sistem automat de detecţie şi stingere a incendiilor. Lipsă sistem supraveghere video. Defecţiune hardware.	1	3	7	Anexă 1
Personalul şi activităţi operaţiuni	Sistem operaţiuni / Staţie de lucru / bază de date / sisteme informatice importante	3	servicii necorespunzătoare de suport pentru sisteme	Neconformitatea cu reglementările legale respective (resurse umane, PSI, autorizări / avizări autorităţi locale)	1	3	7	Anexă 1
Personalul şi activităţi Fin-ctb	Sistem financiar-contabil Staţie de lucru / bază de date sisteme informatice importante	2	fraude şi activităţi criminale externe	Lipsa verificărilor eficace. Lipsa principiului celor patru ochi. Management impropriu de acces în aplicaţie.	1	3	6	Anexă 1
Personal şi sisteme IT	Staţie de lucru / bază de date sisteme informatice importante	2	expuneri externe ale securităţii sistemelor	Lipsă sistem automat de detecţie şi stingere a incendiilor. Lipsă sistem supraveghere video. Defecţiune hardware.	1	3	6	Anexa 1

Tratarea riscurilor 2024

Evaluare internă a riscurilor operaţionale

(măsuri de control ale riscurilor propuse pentru reducerea riscurilor)

ANEXA 1 la registrul riscurilor

A – Probabilitatea producerii evenimentelor

B – Nivel impact

C – Nivel risc

Nr. crt	Eveniment nedorit	Ameninţare	Vulnerabilitate asociată	A	B	C	Măsuri de control al riscului
1.	Producerea unui incendiu	Incendiu	Absenţa unui sistem automat de detecţie şi stingere a incendiului	Mică	Mare	Mediu	**Implementate** Verificarea şi întreţinerea instalaţiilor Existenţa procedurilor de creare a fişierelorde back-up care vizează frecvenţa, tipul de back-up, persoanele autorizate şi verificarea periodică Instruirea personalului autorizat al sistemului privind modul de acţiune la incendiu. **Măsuri viitoare** Existenţa unor mijloace automate de detecţie şi stingere a incendiului Realizarea unor contracte de furnizare echipamente de calcul, birotică, în cazul producerii unor astfel de Existenţa unui spaţiu alternativ de reluare a activităţii ptr personal.
2.	Producerea unui cutremur	Cutremur	Lipsa planurilor de continuare a activităţii sau a procedurilor de recuperare / refacere a informaţiilor în caz de cutremur	Mică	Mare	Mediu	**Implementate** Structura de rezistenţă a clădirii este solidă. Pereţii exteriori şi despărţitori ai camerelor în care sunt instalate echipamentele sistemului sunt din materiale solide. Existenţa locaţiei alternative de procesare a datelor. **Măsuri viitoare** Instruirea personalului autorizat al sistemului privind modul de acţiune în caz de cutremur. Realizarea unor contracte de furnizare echipamente de calcul, birotică, în cazul producerii unor astfel de evenimente.
3.	Alimentare necores-punzătoare cu energie electrică	Căderi ale tensiunii de alimentare	Lipsa surselor neîntreruptibile de alimentare cu energie electrică	Mică	Mare	Mediu	**Implementate** Servere de back-up se află într-o locaţie separată toate calculatoarele sunt prevăzute cu ups **Măsuri viitoare** Implementare replicare sincronă între sediul central şi datacenter Achiziţionare generator electric

4.	Copierea neautorizată de date / software	Dezvăluire Informații	Acces neautorizat – Copierea neautorizată de date / software	Mică	Mare	Mediu	**Implementate** Existența antivirus, Firewall Instruirea continuă a personalului Backup periodic al datelor în data center conform procedurilor operaționale existente **Măsuri viitoare** Utilizatorii cu drepturi de acces limitate ai sistemului trebuie să aibă o pregătire corespunzătoare privind utilizarea resurselor și serviciilor sistemului De asemenea, trebuie respectată politica de securitate existentă
5.	Utilizarea necores-punzătoare a resurselor și serviciilor sistemului (erori de Utilizare)	Erori de operare ale personalului	Configurarea necorespunzătoare a funcțiilor de securitate ale sistemelor de operare	Mică	Mare	Mediu	**Implementate** S-a creat o locație alternativă de backup. Toate update-urile pe aplicațiile software se testează pe mediul de te înainte de implementarea în mediul de producție **Măsuri viitoare** Elaborarea unei politici 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. Elaborarea unei proceduri 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.
			Lipsa fișierelor de back-up	Mică	Mare	Mediu	
			Pregătire de specialitate necorespunzătoare a personalului	Mică	Mare	Mediu	
		Erori de programare	Configurarea necorespunzătoare a funcțiilor de securitate ale sistemelor de operare	Mică	Mare	Mediu	
			Lipsa fișierelor de back-up	Mică	Mare	Mediu	
			Pregătire de specialitate necorespunzătoare a personalului	Mică	Mare	Mediu	
		Modificări neautorizate ale Software-ului	Lipsa fișierelor de back-up	Mică	Mare	Mediu	
			Pregătire de specialitate necorespunzătoare a personalului	Mică	Mare	Mediu	

6.