GRUPUL MEDLIFE
Politica de gestionare a riscurilor
Ghidul ERM

Cuprins

POLITICA DE GESTIONARE A RISCURILOR

Scop

Scopul prezentei politici de gestionare a riscurilor este de a stabili o abordare structurată și consecventă pentru identificarea, evaluarea, gestionarea, monitorizarea și raportarea riscurilor care pot afecta realizarea obiectivelor strategice, operațiunile, activele, reputația sau obligațiile de conformitate ale organizației. Această politică asigură că gestionarea riscurilor este o parte integrantă a tuturor proceselor decizionale din cadrul organizației.

Domeniu de aplicare și aplicabilitate

Prezenta politică se aplică tuturor activităților desfășurate de entitățile juridice ale Grupului MedLife (denumit în continuare „Grupul"), astfel cum sunt prezentate în situațiile financiare consolidate, precum și oricărei alte entități juridice care va deveni parte a Grupului în viitor. Politica poate fi pusă la dispoziția angajaților, personalului nesalarizat, pacienților și clienților, precum și tuturor părților interesate externe relevante, inclusiv contractanților și furnizorilor de servicii, pentru a asigura transparența și alinierea pe tot parcursul procesului de implementare. Aceasta acoperă toate tipurile de riscuri, inclusiv, dar fără a se limita la: riscuri strategice, operaționale și financiare (inclusiv riscurile de sustenabilitate incluse în oricare dintre rubricile anterioare).

Alinierea la reglementări și standarde

Gestionarea riscurilor este o componentă esențială a bunei guvernanțe. **Gestionarea globală a riscurilor (Enterprise Risk Management - ERM)** are ca scop păstrarea și îmbunătățirea continuă a valorii, reputației și motivației interne a Grupului. Aceasta încurajează un nivel rezonabil de asumare a riscurilor, acceptabil pentru părțile interesate și suportabil din punct de vedere economic. Atingerea acestui obiectiv se bazează pe o bună înțelegere a riscurilor noastre și pe abilitățile de a le gestiona. Prezenta politică a fost elaborată ținând seama de standardele de guvernanță și conformitate aplicabile la momentul redactării, inclusiv, dar fără a se limita la:

- ISO 31000
- Cadrul COSO ERM

Politica se aplică în conformitate cu toate legislațiile și reglementările naționale și europene relevante aplicabile operațiunilor Grupului și ale filialelor sale.

Guvernanță și responsabilități

Prezenta politică a fost elaborată sub coordonarea Departamentului Financiar din cadrul MedLife S.A. și a fost aprobată oficial de către directorul general al companiei.

În cadrul Grupului MedLife, Divizia Financiară sprijină conducerea de linie în implementarea, monitorizarea și îmbunătățirea continuă a Politicii de gestionare a riscurilor. Aceasta se asigură că toate riscurile — inclusiv riscurile de mediu, sociale și de guvernanță (ESG) — sunt identificate, evaluate și integrate în cadrul mai larg de gestionare a riscurilor al Grupului.

Obiective

Obiectivele acestei politici sunt:

- Promovarea unei culturi proactive de gestionare a riscurilor.
- Minimizarea probabilității și a impactului potențialelor amenințări.
- Îmbunătățirea procesului decizional prin analiza informată a riscurilor.
- Asigurarea conformității cu legile, reglementările și standardele aplicabile.
- Protejarea intereselor părților interesate și a reputației organizației.

Formare și sensibilizare

Organizația va organiza sesiuni periodice de instruire pentru a se asigura că tot personalul relevant înțelege importanța gestionării riscurilor și este familiarizat cu procesele și instrumentele utilizate.

Revizuirea politicii

Prezenta politică va fi revizuită ori de câte ori au loc schimbări organizaționale sau externe semnificative, pentru a asigura relevanța și eficacitatea continuă a acesteia. Toate revizuirile trebuie aprobate de Consiliul de Administrație.

CAPITOLUL 1: ORGANIZAREA GUVERNANȚEI ERM

CRO raportează direct Consiliului de Administrație, conform prevederilor Codului de Guvernanță al BVB.

Contact / membru al rețelei ERM	Responsabilități operaționale	Acțiuni	Rezultate
Directorul de risc (sediul central)	Responsabil pentru exercițiul ERM	• Pregătește și conduce evaluarea anuală • Să fie consultat cu privire la identificarea și evaluarea riscurilor de către entități • Contestarea analizelor de risc efectuate de entități • Coordonează activitatea cu diversele departamente ale sediului central • Elaborarea și menținerea cadrului și a metodologiei de gestionare a riscurilor. • Facilitează evaluările de risc și asigură aplicarea consecventă a politicii. • Oferirea de programe de instruire și de sensibilizare privind riscurile	Analiza finală a riscurilor la nivel de grup
Consiliul de administrație (Sediul central)	Aprobă politica de gestionare a riscurilor Definește apetitul la risc Aprobă analiza anuală a riscurilor	• Validează analiza anuală a riscurilor • Ajustarea apetitului la risc și a nivelurilor de toleranță • Analizează periodic expunerile la riscuri majore și planurile de atenuare	
Departamente funcționale (Sediul central)	Definește șabloanele de evaluare a riscurilor Sprijin pentru planurile de acțiune	• Identificarea riscurilor • Definirea liniilor directoare pentru evaluările de risc realizate de departamentele lor • Oferirea unei „a doua opinii” • Implementarea măsurilor și a acțiunilor de control • Contribuția la pregătirea analizei de risc a Grupului	Linii directoare pentru evaluarea riscurilor
Director financiar (Sediul central)	Responsabil pentru riscuri și acțiuni de atenuare	• Să fie informat cu privire la sinteza riscurilor și la implementarea managementului global al riscurilor	

Trebuie subliniat faptul că **Consiliul de administrație al Grupului** este responsabil de validarea analizei finale a riscurilor prezentată de CRO și pre-validată de Comitetul executiv.

CRO are datoria de a „spune care sunt riscurile” și supraveghează dezvoltarea competențelor și maturității în materie de gestionare a riscurilor în cadrul Grupului.

CAPITOLUL 2: METODOLOGIA DE GESTIONARE A RISCURILOR

Acest capitol descrie abordarea privind gestionarea riscurilor:

- Contextul
- Evaluarea riscului:
  - ✓ Identificarea
  - ✓ Analiza cauzelor și a consecințelor
  - ✓ Evaluarea pe baza scenariilor
- Stabilirea riscului țintă
- Stabilirea strategiei de atenuare și a planurilor de acțiune
- Monitorizarea și revizuirea riscurilor

2.1 Contextul afacerii

Primul pas în gestionarea riscurilor este înțelegerea activităților entității, a mediului în care aceasta operează și a elementelor sau evenimentelor interne/externe care ar putea să o pună în pericol.

Pentru a face acest lucru, CRO colectează diverse tipuri de informații:

- în cadrul Grupului: revizuirea evenimentelor anterioare, analiza obiectivelor strategice, financiare și operaționale, identificarea părților interesate etc.,
- în afara Grupului: analiza tendințelor din industrie, compararea cu companii similare etc.

2.2 Evaluarea riscului

2.2.a. Identificarea

CRO trebuie să aibă o înțelegere aprofundată a problemelor cu care se confruntă entitatea (sau entitățile) și/sau țara (sau țările) aflate în perimetrul său (al acestora). Următoarele acțiuni vor contribui la colectarea diferitelor surse de informații pentru a identifica/distinge riscurile cele mai amenințătoare pentru entitate:

- să desfășoare interviuri periodice (cel puțin anual) cu membrii CA sau ai Comitetului Executiv al entității sale, fie individual, fie prin intermediul unor comitete ad-hoc, precum și cu alți manageri operaționali
- să interacționeze cu diferiții manageri de linie funcțională din cadrul entității
- să colaboreze cu o echipă multidisciplinară la diferite niveluri ale entității, pentru a efectua o analiză a riscurilor emergente sau a riscurilor legate de noi activități,
- să utilizeze *Catalogul de riscuri* ca bază de lucru pentru identificarea riscurilor, care enumeră majoritatea categoriilor de riscuri întâlnite în activitățile Grupului, deși nu este în niciun caz exhaustiv. În special, catalogul poate fi utilizat pentru a verifica dacă anumite riscuri generale au fost luate în considerare în cadrul revizuirii.

2.2.b Analiza cauzelor și consecințelor

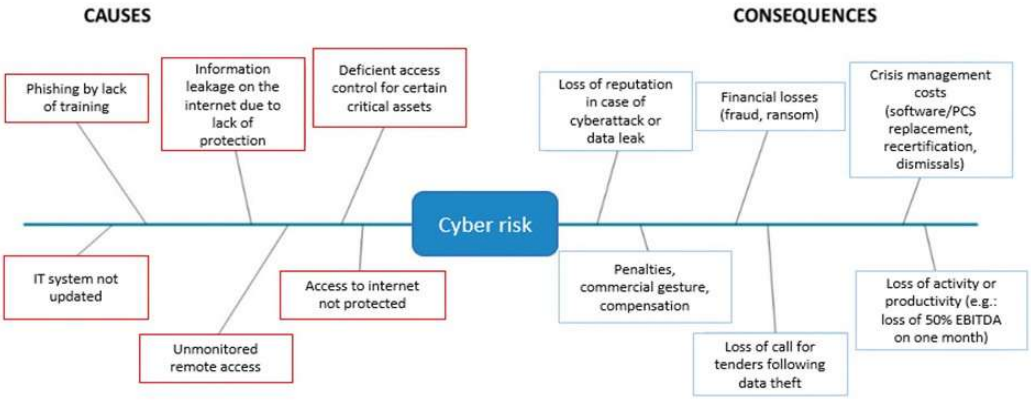
Apariția riscului este generată de una sau mai multe cauze și conduce la una sau mai multe consecințe.

Cauzele pot fi directe (declanșând direct apariția riscului) sau indirecte (favorizând apariția riscului, în amonte în lanțul cauzal, și/sau amplificând amploarea consecințelor sale).

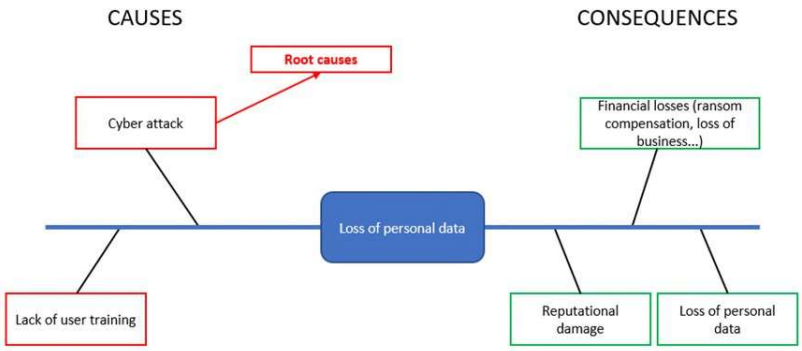
Există mai multe metodologii disponibile pentru efectuarea acestei analize și identificarea cauzelor (diagrama Ishikawa sau arborele cauzelor, cele 5 întrebări „de ce", etc.): MedLife utilizează în mod standard arborele cauzelor, care este potrivit pentru cele mai simple analize. Este important să se caute cauzele principale pentru a crește eficacitatea măsurilor de atenuare.

Consecințele vor genera impacturi asupra companiei. Este esențial să le identificăm corect: dacă nu se acționează asupra cauzelor, care sunt uneori externe, acțiunea asupra consecințelor poate limita impactul la proporții acceptabile sau neglijabile pentru companie.

Exemplul 1: Exemplu de diagramă Ishikawa care ilustrează riscurile cibernetice



În cazul riscurilor corelate, consecința unui risc poate fi, de asemenea, cauza altuia. Faptul că un eveniment este o cauză sau o consecință depinde de perspectiva din care este privit. În exemplul de mai jos, cauza aparentă a pierderii datelor cu caracter personal a fost un atac cibernetic: trebuie să urcăm înapoi pe arborele cauzelor pentru a identifica cauzele principale, care ar putea fi, de exemplu, o defecțiune a sistemelor de securitate sau de control al accesului.



Exemplul 2: Exemplu de diagramă Ishikawa care ilustrează riscul de nerespectare a legislației privind protecția datelor

2.2. Evaluarea riscului pe baza scenariilor

Odată identificate riscurile, împreună cu cauzele și consecințele acestora, ele trebuie evaluate din două perspective:

- **impact** și
- **probabilitate**,

  folosind un scenariu (adică un set de ipoteze privind apariția riscului și consecințele acestuia).

Un risc inerent este materializarea unui pericol: într-un mediu necontrolat, parametrii săi (probabilitate și impact) depind exclusiv de natura pericolului și de mediul în care are loc evenimentul.

- **Riscul inerent (sau brut) are, în general, parametri ridicați.** Se iau măsuri continue (tehnice, organizaționale, de asigurare etc.) pentru a reduce acești parametri.
- **Riscul rezidual (sau net):** Nivelul parametrilor care rezultă din aceste măsuri este cel al riscului rezidual: acest nivel al riscului rezidual constituie obiectul sistemului global de gestionare a riscurilor.
- **Riscul țintă:** Pentru fiecare risc identificat, CRO determină un nivel de risc țintă, precizând expunerea sau asumarea de risc pe care o acceptă, în conformitate cu legea și apetitul la risc definit de Grup. Acesta

este caracterizat de un nivel țintă de impact și probabilitate sau definit de indicatori financiari sau nefinanciari.

Scenarii de risc

Un risc este evaluat pe baza unui **scenariu standard**, a cărui descriere permite definirea ipotezelor pentru cuantificarea impactului și probabilității riscului și obținerea coerenței între acești parametri. Această evaluare se bazează pe două aspecte:

- Riscul **inerent**: înainte de implementarea planurilor de atenuare sau în cazurile în care sunt deja în vigoare acțiuni în curs, având în vedere că acestea sunt ineficiente
- Risc **rezidual**: după punerea în aplicare a planurilor de atenuare care includ măsuri continue și planuri de acțiune specifice

Deși descrierea riscului poate fi generală, scenariul trebuie să fie detaliat și să ia în considerare caracteristicile specifice ale riscului (contextul local, proiectul/activul în cauză, ipotezele de materializare etc.) pentru o evaluare adecvată.

Deși evaluările de risc trebuie să fie reprezentative, nu este necesar ca acestea să fie foarte precise. Ordinea de mărime este suficientă pentru a determina dacă riscul este potențial catastrofal sau, dimpotrivă, minim.

Orizontul de timp (sau de apariție) al riscului corespunde perioadei în care este probabil ca riscul să se producă. Acesta este strâns legat de scenariul selectat.

- **Pe termen scurt:** riscul se produce în termen de 1-3 ani,
- **Termen mediu:** riscul se produce în 4-6 ani,
- **Pe termen lung:** riscul se materializează după o perioadă de peste 6 ani.

Definirea unui **scenariu extrem** poate contribui la testarea rezilienței orientărilor strategice și a deciziilor de investiții ale Grupului și permite estimarea gradului de pregătire în raport cu anumite riscuri rare, atât în ceea ce privește prevenirea, cât și atenuarea. Scenariul extrem se bazează pe accidente sau evenimente de referință considerate rare, dar nu imposibile.

Impact financiar și nefinanciar

Impactul financiar reprezintă costul pentru entitate pe durata scenariului. Acesta este evaluat pe o scară de 4 niveluri, de la 1 pentru impactul cel mai redus la 4 pentru impactul cel mai catastrofal. Prin convenție, acesta este comparat cu o cantitate de referință, care este, în general, EBITDA cumulată pe durata perioadei de referință a Grupului (Planul pe termen mediu).

Scor	Nivelul impactului	Interval de valori (% din valoarea de referință, EBITDA cumulată pe o perioadă de 3 ani)
1	Nesemnificativ	< 1%
2	Minor	Între 1% și 3%
3	Moderat	Între 3% și 5%
4	Major	Între 5% și 15%
5	Catastrofal	>= 15%

Impactul financiar al riscului inerent este exprimat/evaluat ca valoare suplimentară/abatere față de scenariul de bază bugetat.

Se vor analiza toate impacturile, specificându-se natura acestora (EBITDA, sub EBITDA, valoarea activelor, CAPEX etc.).

Pentru o înțelegere clară a evaluării riscului rezidual și a evoluției acestuia, va fi necesar:

- formalizarea principalelor ipoteze de bază incluse în bugetul de referință și în modelarea pentru anii următori;
- să se indice partea inclusă în „provizioane” în buget.

Exemplu de calcul al impactului: Riscul cibernetic: un total de 151 milioane EUR pentru riscul inerent, defalcat astfel:

- *Costul gestionării crizei: 84 milioane EUR*
- *Pierderea de venituri: 40 de milioane EUR*
- *Distrugerea activelor (stații de lucru): 2 milioane EUR*
- *Despăgubiri comerciale: 25 milioane EUR*

Asigurarea acoperă o parte din costul gestionării crizei, pierderea de venituri și distrugerea activelor. Impactul financiar al riscului rezidual este redus la 85 de milioane de euro.

Impactul nefinanciar

Impactul nefinanciar reprezintă măsurarea consecințelor pentru Grup (și, după caz, pentru părțile interesate) ale aspectelor nefinanciare, cum ar fi:

- resurse umane,
- reputația sau imaginea Grupului,
- mediul,
- juridice,
- sociale sau societale,
- sănătate și siguranță.

Impactul nefinanciar este evaluat pe o scară de 5 niveluri, de la 1 pentru cel mai redus impact până la 5 pentru cel mai catastrofal.

Scor	Nivelul impactului	**Descriere** (*poate rezulta cel puțin unul dintre criteriile de mai jos)*
1	Foarte scăzut	Niciun impact sau impact nesemnificativ asupra sănătății umane (*accident de muncă urmat de modificarea posturilor/tratament medical/efect moderat asupra sănătății*) sau asupra mediului (*poluare minoră cu impact pe termen scurt (până la 3 luni)*). Situația poate fi rezolvată pe termen scurt. Acoperire mediatică locală sau de nivel redus. Acțiuni civile/comerciale cu impact financiar și/sau asupra reputației limitat.
2	Redus	Un anumit impact asupra sănătății umane (*leziuni grave sau severe: accident cu pierdere de timp (LTA) / fără efect semnificativ asupra sănătății*) sau asupra mediului (*poluare minoră cu un impact localizat pe termen mediu (până la un an)*). Amenințare reală la adresa stabilității structurii. Acoperire mediatică locală, regională sau națională limitată. Acțiune civilă/comercială cu impact financiar și/sau asupra reputației limitat.
3	Moderat	Impact de lungă durată sau ireversibil asupra sănătății umane (*leziuni grave sau severe: accident cu pierdere de timp (LTA) / efect semnificativ asupra sănătății*) sau asupra mediului (*poluare moderată cu impact localizat pe termen mediu (până la un an)*). Amenințare reală la adresa stabilității structurii. Acoperire media regională sau națională. Acțiuni în justiție în materie civilă/comercială cu impact financiar și/sau reputațional semnificativ.
4	Grav	Impact ridicat asupra sănătății și vieții umane (un deces, vătămări grave/efecte asupra sănătății/invaliditate pe termen lung) sau asupra mediului (poluare gravă cu impact localizat care durează până la 2 ani. Costuri semnificative de igienizare) Continuitatea structurii este pusă în pericol. Acoperire mediatică extinsă. Posibilitatea unor acțiuni în justiție împotriva conducerii companiei.
5	Catastrofal	Impact ridicat asupra sănătății și vieții umane (*mai multe decese cauzate de același eveniment*) sau asupra mediului (*poluare majoră cu modificări pe termen lung ale mediului, daune ireversibile*). Continuitatea structurii este grav compromisă. Acoperire mediatică majoră și campanie de presă negativă susținută. Acțiune în justiție împotriva consiliului de administrație sau a conducerii companiei

Probabilitate

În absența statisticilor sau a unor reguli specifice ale Grupului, probabilitatea poate fi estimată printr-o combinație de factori: evenimentele care au avut loc, eficacitatea măsurilor de atenuare existente (evaluate folosind indicatori), bunul simț, experiența etc. Se recomandă combinarea mai multor puncte de vedere și a mai multor surse de date. Explicarea factorilor care au condus la această estimare va facilita înțelegerea acesteia.

Probabilitatea de apariție este evaluată pe o scară de 4 niveluri, de la 1 pentru intervalul de probabilitate cel mai scăzut la 4 pentru cel mai ridicat:

Scor	Nivel de probabilitate	Interval de valori	Comentariu privind semnificația
1	Rar	< 5%	Există o probabilitate foarte mică, dar nu neglijabilă, ca riscul să se materializeze.
2	Puțin probabil	5% - 25 %	Există o posibilitate ca riscul să se materializeze.
3	Posibil	15%–25%	Există o probabilitate moderată ca riscul să se materializeze.
3	Probabil	25 și 50 %	Există o posibilitate clară ca riscul să se materializeze, care este mai mică decât probabilitatea ca riscul să nu se materializeze.
4	Cert	>= 50 %	Este mai probabil ca riscul să se materializeze decât să nu se materializeze.

Atunci când probabilitatea unui risc depășește 50 %, este recomandabil să se ia în considerare includerea integrală sau parțială a impactului acestuia în buget/previziuni.

Evenimentele de risc recurente sunt riscuri care pot apărea în fiecare an, cu aceeași probabilitate și același impact. Este vorba despre evenimente specifice despre care știm că vor avea loc probabil, fără a ști însă de câte ori pe durata orizontului de bugetare. În mod implicit, astfel de riscuri trebuie evaluate în primul an al perioadei de bugetare (de exemplu: riscul de credit, riscul de indisponibilitate a anumitor active, riscul de securitate cibernetică, riscul legat de resurse umane etc.)

2.3 Stabilirea strategiei țintă de atenuare a riscurilor și a planurilor de acțiune

Apetitul la risc este definit ca tipul și nivelul de risc pe care Grupul este pregătit să îl accepte ca parte a strategiei sale de creare de valoare.

Acesta este exprimat în termeni de variații acceptabile sau ținte pentru indicatori:

- **valori financiare,** cum ar fi capitalul angajat, EBITDA,
- valori **nefinanciare,** cum ar fi reputația în rândul părților interesate,
- **indicatori** nefinanciari: rata de disponibilitate, rata de satisfacție, rata accidentelor etc.,
- limite **de expunere** sau **praguri de alertă** legate de criteriile definite (de exemplu, valoarea maximă a capitalului angajat pe țară, volumele neacoperite în cazul riscurilor de piață, franșiza de asigurare etc.).

Aceste criterii și limite sunt definite în politici specifice de risc, care precizează, de asemenea, gestionarea riscului în anumite domenii, procedurile de gestionare a riscului și indicatorii de monitorizare.

Apetitul la risc se poate modifica în timp, pe măsură ce mediul și obiectivele Grupului evoluează.

2.4 Strategia de atenuare a riscurilor și planurile de acțiune

Pentru fiecare risc, conducerea numește un **responsabil**: această persoană este însărcinată cu definirea strategiei de gestionare a riscului, precum și cu elaborarea și punerea în aplicare a planurilor de acțiune menite să atingă nivelul de risc țintă.

Planurile de acțiune ar trebui să vizeze cauzele riscului, pentru a reduce **probabilitatea** acestuia, sau **consecințele** riscului, pentru a reduce **impactul** acestuia.

Strategia de atenuare reprezintă abordarea globală adoptată pentru a gestiona riscul. Aceasta poate fi foarte variată. Ea va fi cu atât mai eficientă cu cât a fost aleasă, elaborată și adaptată în mod conștient la contextul entității și la riscul respectiv, mai degrabă decât să fie rezultatul unei sume de inițiative coordonate în mod disparat.

- **Eliminarea riscului.** Încetarea activității, a activelor sau a relațiilor cu o parte interesată.
- **Reducerea riscului** prin:

✓ **Diversificarea riscului**: repartizarea riscului pe mai multe activități sau domenii independente a priori pentru a elimina efectul de concentrare. De exemplu, diversificarea prezenței geografice a Grupului pentru a reduce riscul de țară. Trebuie remarcat faptul că diversificarea are un efect puternic, dar poate eșua în cazul riscurilor dependente, în special în cazul riscului sistemic.

✓ **Implementarea măsurilor** de **control** (prevenire, protecție, dezvoltarea controlului intern), înainte și după procesare etc. De exemplu, implementarea separării sarcinilor pentru a reduce riscul de fraudă.

- **Transferul riscului**. Asumarea consecințelor riscului de către o terță parte. În majoritatea cazurilor, se transferă doar o parte din risc. De exemplu: asigurarea (plata unei prime în schimbul unei despăgubiri în cazul unei cereri de despăgubire), transferul către bănci în cazul împrumuturilor, măsuri contractuale cu clienții sau furnizorii. Responsabilitatea poate fi transferată parțial prin delegarea autorității sau prin contract, dar nu și responsabilitatea principală către client. Termenul „responsabilitate partajată" este mai adecvat. Trebuie remarcat faptul că impactul asupra imaginii, impactul juridic și impactul asupra resurselor umane nu sunt, în general, transferate către terți, deoarece acestea afectează răspunderea companiei.
- **Împărțirea riscului**. Riscul poate fi, de asemenea, împărțit cu asociații sau partenerii: de exemplu, partenerii locali care vor împărți riscurile operaționale într-un proiect de construcții sau co-acționarii dintr-o societate mixtă.
- **Acceptarea riscului.** A nu face nimic este o opțiune posibilă. Totuși, aceasta presupune că nivelul de risc poate fi evaluat și menținut în limite acceptabile, iar planul de acțiune este eficient și adecvat. Această abordare este cunoscută și sub denumirea de „retenție a riscului".

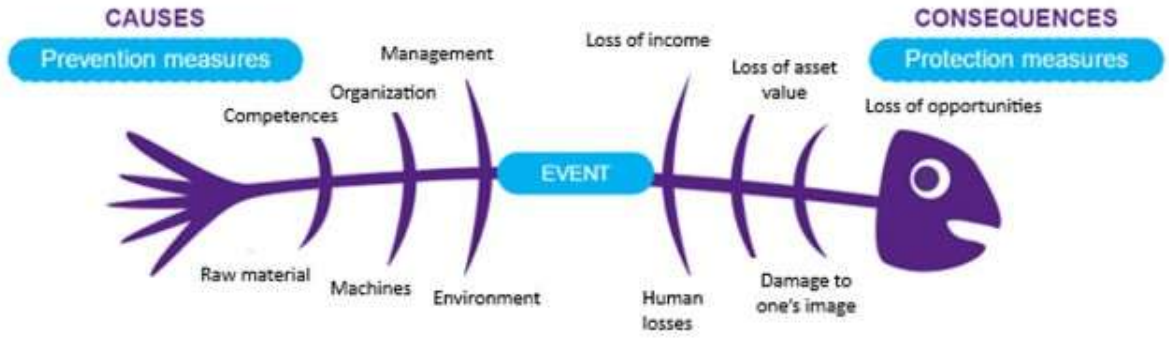
Riscurile strategice sunt riscuri legate de noțiunea de antreprenoriat. Acestea nu pot fi reduse sau transferate la fel ca riscurile operaționale.

De asemenea, pot fi gestionate prin inovare, adaptarea modelelor de afaceri, activități de lobby, informații economice și dezvoltarea competențelor, de exemplu.

Strategia de atenuare este adesea o combinație a diverselor strategii de bază.

Uneori, Grupul poate opta pentru alte strategii de atenuare: creșterea riscului (prudență excesivă în trecut, schimbări de context, de tehnologie etc.), adaptarea modelului său de afaceri etc.

În funcție de strategia de atenuare aleasă, se vor defini și pune în aplicare planuri de acțiune pentru atingerea nivelului de risc țintă. Acest demers se va baza pe o analiză a cauzelor și a consecințelor, în vederea selectării măsurilor adecvate:



Pertinența planului de atenuare trebuie să țină seama de raportul cost/beneficiu: conducerea poate fi astfel determinată să accepte un risc dacă costul atenuării acestuia este considerat prea ridicat în raport cu beneficiul preconizat.

În cele din urmă, atunci când incertitudinea sau măsurile puse în aplicare pot avea un aspect pozitiv, este important să se țină seama de acest lucru pentru a adapta atenuarea și nivelul țintă. Planurile de acțiune și planurile de atenuare pot crea, de asemenea, **oportunități** care depășesc reducerea nivelului de risc. În acest caz, descrierea riscului va fi completată cu o descriere a oportunității asociate.

2.4 Monitorizarea şi revizuirea riscurilor

Planul de atenuare constă în:

- măsuri continue menite să reducă riscul inerent la nivelul riscului rezidual, precum și
- acțiuni specifice, definite în timp, care permit reducerea riscului inerent la nivelul riscului rezidual și, în unele cazuri, aducerea nivelului riscului rezidual la nivelul riscului țintă.

Progresul unui plan de atenuare trebuie să fie măsurabil în mod obiectiv: prin urmare, indicatorii cantitativi sau etapele-cheie de progres trebuie definiți la momentul punerii în aplicare a planului de atenuare și trebuie să facă obiectul unor evaluări periodice ale progresului.

În plus, se recomandă instituirea unui sistem care să permită evaluarea eficacității efective a planului de atenuare, ținând seama de evoluția indicatorilor utilizați pentru evaluarea expunerii la risc.

Recomandăm utilizarea indicatorilor operaționali existenți (de exemplu, rata de satisfacție a clienților, rata de disponibilitate a activelor, sondaje de opinie, indicatori financiari etc.).

Auditul intern, controlul intern și departamentul de gestionare a riscurilor pot fi consultate în mod util pentru a oferi o opinie cu privire la calitatea și eficacitatea planului de atenuare.

În concluzie, un plan de atenuare eficient necesită definirea/punerea în aplicare a:

- un obiectiv de risc țintă,
- identificarea principalilor factori de risc și definirea unei strategii de atenuare corespunzătoare,
- un proiect-pilot pentru fiecare acțiune în vederea atingerii nivelului de risc țintă,
- monitorizarea punerii în aplicare a planurilor de atenuare.

Calitatea și eficacitatea planului de atenuare pentru fiecare risc sunt evaluate pe o scară de patru puncte, după cum urmează:

Calitate	Strategia decisă	Strategie implementată	Comentariu
De (re)construit	Nu	Nu	Acest lucru poate fi valabil în cazul unui risc nou sau dacă expunerea la risc s-a modificat semnificativ. Strategia de gestionare a riscurilor nu a fost încă definită sau redefinită.
Scăzut	Da	Nu	Acest lucru se poate întâmpla în cazul unui risc care a fost deja identificat, dar a cărui amploare sau natură s-a modificat. Strategia este definită, dar nu a fost pusă în aplicare. Planul de atenuare sau sistemul de monitorizare nu a fost încă pus în aplicare.
Perfectibil	Da	Parțial	Există un plan de atenuare, dar acesta nu este suficient pentru riscul vizat sau nu este încă implementat pe deplin.
Bun	Da	Da	Planul de atenuare definit este suficient și adecvat pentru atingerea riscului țintă. Planul de tratare și sistemul de monitorizare sunt implementate.

CAPITOLUL 3: UN ERM OPERAȚIONAL

Pentru revizuirea ERM, în cadrul organizațiilor sunt utilizate două abordări combinate:

- Abordarea „de sus în jos” este un flux de informații strategice care pornește de la viziunea Consiliului de administrație / Conducerii executive: aceasta structurează viziunea asupra riscurilor și oferă orientările generale care trebuie luate în considerare de entitățile operaționale în activitatea lor;

  CRO organizează un exercițiu de identificare a macro-riscurilor Grupului, începând cu o revizuire a sintezei riscurilor Grupului de către Consiliu și continuând cu un exercițiu „de sus în jos” sub forma unor interviuri sau sesiuni de brainstorming cu membrii Comitetelor executive.

  Sunt evidențiate cele mai importante riscuri asupra cărora conducerea dorește să aibă o imagine de ansamblu, inclusiv scenariile de risc și planurile de atenuare.

- Abordarea „de jos în sus” reprezintă un flux de informații operaționale bazat pe viziunea entităților/operațiunilor de pe teren: acestea raportează riscurile legate de situații operaționale specifice.

Implementarea în primul an

Organizat de CRO / CFO la sediul central, acest **Kick-Off** formalizează începutul procesului de analiză a riscurilor. Instrucțiunile de analiză a riscurilor ale Grupului sunt apoi trimise filialelor:

- liniile directoare specifice stabilite de Comitetul Executiv și revizuite de Comitetul de Audit al Grupului pentru primul an. Acestea pot conduce la examinarea mai aprofundată a anumitor riscuri sau categorii de riscuri din motive ciclice;
- riscurile identificate în timpul analizei de sus în jos;
- instrucțiunile specifice de analiză a riscurilor definite de diferite funcții (de exemplu, resurse umane, juridic GDPR, IT), linii de apărare (Audit Intern).

Schimburi cu diversele filiale și CRO

În timpul revizuirii, este esențial ca CRO să mențină o comunicare regulată cu diverse persoane de contact din cadrul entității sale, în special:

- diferitele „funcții" și activități operaționale, pentru a identifica riscurile, a realiza cea mai bună evaluare posibilă a riscurilor inerente și reziduale și a defini scenarii de risc, precum și pentru a analiza critic planurile de acțiune propuse de conducere,
- celelalte linii de APĂRARE (control intern, audit intern) pentru a contribui la evaluarea eficacității și a impactului planurilor de acțiune,
- pentru a ține CEO-ul la curent cu progresul revizuirii.

Notă: Se recomandă documentarea evaluărilor în aceleași formate cât mai curând posibil. Toate detaliile de cuantificare sunt realizate imediat ce datele necesare sunt disponibile.

Dacă este necesar, CRO poate agrega riscurile de aceeași natură, care au aceleași cauze (pentru a reuni o pârghie comună de prevenire) sau aceleași consecințe (pentru a reuni o pârghie comună de protecție) sau pentru a grupa anumite riscuri de importanță redusă, dar recurente în mai multe entități (riscuri care au aceleași probleme de afaceri sau același responsabil de risc identificat).

Sinteza riscurilor Grupului

Scopul analizei de risc este de a permite Consiliului de administrație sau Comitetului executiv al entității:

- valideze expunerea globală la risc (pe termen scurt, mediu și lung) pe care entitatea o acceptă în lumina obiectivelor sale, a politicilor Grupului privind apetitul la risc și a schimbărilor din mediul său,
- gestioneze principalele riscuri prin monitorizarea evoluției acestora, punerea în aplicare a planurilor de atenuare și desemnarea responsabililor de risc,
- să evalueze eficacitatea planurilor de atenuare și să decidă dacă este necesară adaptarea acestora,
- identifice riscurile emergente la nivel de entitate și de țară,
- informarea părților interesate cu privire la aceste riscuri,
- comunicarea culturii de risc la toate nivelurile organizației.

Rezultatul final este, de asemenea, prezentat Consiliului de administrație și Comitetului de audit în cadrul unei ședințe la care participă CRO, CFO și CEO-ul entității.

Prioritizarea și selectarea riscurilor care trebuie luate în considerare în cadrul revizuirii

Odată finalizată analiza riscurilor individuale și în vederea pregătirii evaluării riscurilor entității, directorul responsabil cu gestionarea riscurilor (CRO) stabilește ordinea de prioritate a riscurilor și le selectează pe cele care vor beneficia de o atenție specială.

Se recomandă selectarea unui număr maxim de riscuri la nivel de entitate (corespunzător unui Top 10 sau Top 15) și la nivel de țară, pentru a facilita înțelegerea analizei de risc și stabilirea priorităților planurilor de acțiune.

Se recomandă ca Comitetul executiv să poarte o dezbatere informată, bazată pe criterii obiective:

- **Impactul financiar** asupra rezultatelor,
- **Impactul nefinanciar**, în special în ceea ce privește părțile interesate,
- **Sustenabilitatea scenariilor extreme**,
- **Evoluția și nivelul gestionării riscurilor** (calitatea și eficacitatea planurilor de atenuare).

De asemenea, acestea răspund nevoilor de conformitate și guvernanță ale societăților cotate la bursă și asigură transparența în comunicarea externă a riscurilor societăților cotate la bursă (raportul anual).

Matricea de risc și imaginea de ansamblu

Matricea de riscuri oferă o imagine de ansamblu asupra tuturor riscurilor pentru un anumit perimetru. Fiecare risc este poziționat pe harta standard de probabilitate/impact. Coordonatele punctului care reprezintă riscul sunt probabilitatea acestuia pe axa x și impactul total pe axa y. Culorile de fundal de pe hartă nu au altă semnificație decât aceea de a ghida cititorul.

LIKELIHOOD	INSIGNIFICANT	MINOR	SIGNIFICANT	MAJOR	CATASTROPHIC
CERTAIN	Low	Moderate	High	Extreme	Extreme
LIKELY	Low	Moderate	High	High	Extreme
POSSIBLE	Low	Moderate	Moderate	High	High
UNLIKELY	Low	Low	Moderate	Moderate	Moderate
RARE	Low	Low	Low	Low	Low

IMPACT

Matricea vă permite să:

- să pună toate informațiile în perspectivă într-un format grafic,
- identifică cele mai semnificative riscuri prin prezentarea unui rezumat transversal al riscurilor clasificate în ordinea importanței la un moment dat,
- obține o înțelegere mai profundă a riscurilor și, dacă este necesar, identifica efectele dependente sau interconectate (efectul domino) și, astfel, optimiza măsurile de atenuare și planurile de acțiune,
- verificarea adecvării sistemelor de control în raport cu aceste riscuri,
- oferi o bază pentru o comunicare internă eficientă a riscurilor.

Coordonarea procesului de bugetare și a proceselor globale de gestionare a riscurilor

Revizuirea finală a riscurilor entității se efectuează în conformitate cu procesul de bugetare: riscurile sunt cuantificate în raport cu bugetul entității.

- Riscurile cu probabilitate ridicată (>50%) sunt incluse în buget (cel puțin parțial). Cel puțin, acestea ar trebui discutate în cadrul evaluării anuale;
- costurile planurilor de gestionare a riscurilor sunt incluse în buget.

CAPITOLUL 4: CATALOGUL DE RISCURI

Anexa 1: catalogul de riscuri – format Excel. Câteva exemple mai jos.

Riscuri strategice
• Mediul de afaceri / Concurenți • Mediul de reglementare • Reputație și strategie de marketing • Definirea și analiza strategiei generale • Atingerea obiectivelor de dezvoltare • Structura organizațională • Evaluarea investițiilor și a achizițiilor și integrarea post-achiziție
Riscuri financiare
• Ratele dobânzilor și cursurile de schimb • Riscul de lichiditate • Contrapartea financiară și/sau comercială • Pensii și scheme de pensii • Alte riscuri financiare (de depreciere, ...)
Riscuri operaționale
• Eficiența, performanța și menținerea activităților noastre operaționale • Tratamentul pacienților • Infecții • Calitate / Tehnologie • Pierderea competențelor / Retenția / Fluctuația • Implicarea angajaților / stres / dezangajare • Relațiile de muncă / climatul social • Transformarea digitală a proceselor și utilizarea datelor • Securitatea cibernetică a infrastructurilor IT, a sistemelor de control industrial sau a aplicațiilor de afaceri • Disponibilitatea sistemelor informatice interne sau a furnizorilor IT externi • Riscuri fizice legate de schimbările climatice • Dezastre naturale (cu excepția schimbărilor climatice) • Corupția și alte încălcări ale normelor de etică și conformitate • Nerespectarea reglementărilor locale privind confidențialitatea datelor (GDPR) • Achiziții și lanț de aprovizionare • Sănătate și siguranță • Securitate • Gestionarea deșeurilor