

005.334:006.4

MANAGEMENTUL RISCULUI – IDENTIFICARE, EVALUARE ȘI REACȚIE LA RISC

*Drd. Hezy SHAYB,
Universitatea Tehnică a Moldovei,
Director executiv,
Compania „Israel Vehicle Importers
Association”, Israel
shaybhezi@gmail.com*

Noțiunea de risc a fost, dintotdeauna, unul din conceptele-cheie mult studiate în științele economice. Autori renumiți au prezentat și identificat principala diferență dintre noțiunea de risc și incertitudine. Factorul principal prezumă că, în anumite cazuri, riscul poate fi măsurat, în alte cazuri – nu. Se pare că o incertitudine măsurabilă (sau „riscul” propriu-zis este cu mult diferit de cel de neimaginat) nu este deloc o incertitudine. Astfel, am putea asocia gestionarea crizelor cu incertitudinea, în timp ce managementul riscului este un mijloc de abordare cantitativă pentru măsurarea și evaluarea expunerii la evenimente și probabilități cunoscute. Scopul acestui articol este de a oferi o mai bună înțelegere a modului în care riscurile ar trebui identificate, evaluate și a modului în care ar trebui să reacționăm eficient la apariția lor.

Cuvinte-cheie: răspunsul în fața riscului, managementul riscului, evaluarea riscului, restructurarea întreprinderii, standardul ISO 3000.

JEL: D81.

Introducere

Managementul riscului poate fi descris ca fiind procesul de gestionare a riscurilor prin identificarea acestora, evaluarea și, apoi, prin

005.334:006.4

RISK MANAGEMENT – IDENTIFYING, ASSESSING AND RESPONDING TO RISKS

*PhD candidate Hezy SHAYB,
Technical University of Moldova,
Executive Director,
“Israel Vehicle Importers
Association”, Israel
shaybhezi@gmail.com*

Risk has been one of the key concepts studied in economics. Famous authors have identified the main difference between risk and uncertainty. The main factor is that in some cases the risk can be measured, in other cases – not. It seems that a measurable uncertainty, or “risk” itself, is not an uncertainty at all. We could associate crisis management with uncertainty while risk management is a quantitative approach to measure and assess the exposure to known events and probabilities. The aim of this article is to offer a better understanding of how should be risks identified, assessed and responded efficiently and effectively.

Keywords: risk response, risk management, risk assessment, enterprise restructuring, ISO 3000 standard.

JEL: D81.

Introduction

Risk management can be described as the process of handling the risks by first identifying them, then evaluating them, and then minimizing or monitoring them in order to keep them as harmless as possible [3, p. 20]. Risks generally are associated with uncertainty. Within organizations, risks can come from a lot of different uncertain aspects: mar-

minimizarea sau monitorizarea lor, pentru a le menține la un nivel, la care impactul generat de ele să fie minim [3, p. 20]. În general, riscurile sunt asociate cu incertitudinea. În cadrul organizațiilor, riscurile pot surveni sub diferite aspecte: evoluția pieței, eșecuri ale proiectelor, accidente, dezastre ale naturii etc.

Există diferite instrumente, care pot fi utilizate în cazul gestionării riscurilor, în funcție de tipul de risc, cu care se confruntă. În mod ideal, în managementul riscurilor, ar trebui urmat un proces de prioritizare a riscurilor, pentru a putea face față, în primul rând, riscurilor, care prezintă o mare amenințare, pot aduce pierderi și care au o mare probabilitate de apariție.

Importanța evaluării corespunzătoare și a prioritizării riscurilor este semnificativă. Conform acestor acțiuni și, în funcție de exactitatea lor, resursele companiei sunt alocate în vederea minimizării riscurilor survenite.

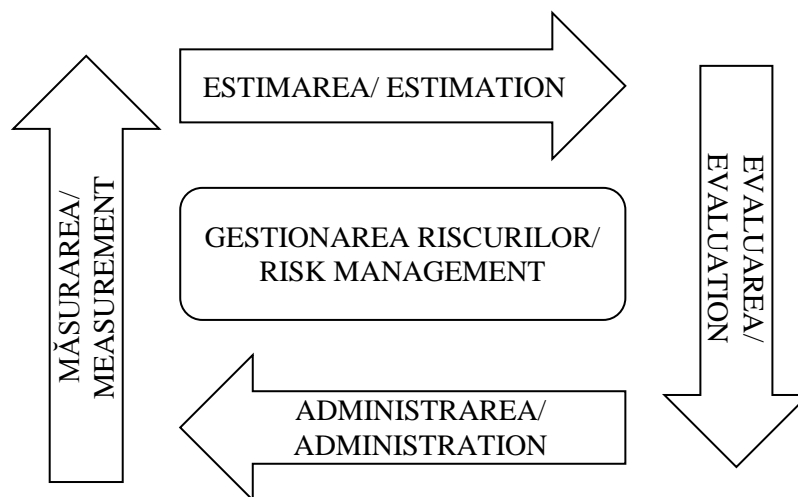
În afară de modelele de management al riscurilor, majoritatea organizațiilor urmează un ciclu de gestionare a riscurilor, prezentat în figura 1.

ket evolution, projects failures, accidents, natural disasters, etc.

There are different tools that can be used when dealing with risks, depending upon the kind of risk faced. Ideally, in risk management, a risk prioritization process should be followed in order to be able to deal first with those risks that present great loss threat and have great probability of occurrence.

The importance of properly assessing and prioritizing the risks is huge. According to this action, and depending on their accuracy, the company's resources are allocated towards minimizing the perceived risks.

Apart from risk management models, typically most of the organizations follow a risk management cycle, as presented in the figure 1.



**Figura 1. Ciclul de gestionare a riscurilor/
Figure 1. Basic Risk Management Cycle**

Sursa: elaborată de autor!

Source: elaborated by the author

În conformitate cu acest ciclu de gestionare a riscurilor, există patru etape în procesul de management al riscurilor:

- Etapa 1. Identificarea riscului;
- Etapa 2. Evaluarea riscului;
- Etapa 3. Gestionarea riscului;
- Etapa 4. Evaluarea impactului riscului.

Prima etapă o constituie identificarea riscurilor și constă în stabilirea sursei acestora. Sursele riscurilor pot fi interne sau externe sistemului. Ambele pot fi controlate doar într-o anumită măsură.

După identificarea riscurilor, acestea trebuie evaluate din punctul de vedere al potențialului lor de a fi dăunătoare companiei. Potențialul se calculează ținând seama de probabilitatea de apariție și impactul estimat. După finalizarea evaluării, trebuie să fie elaborat și implementat planul de gestionare a riscurilor. Acesta definește mecanismele de control, care ar trebui utilizate pentru diminuarea riscului.

Metode, tehnici și etape utilizate în managementul riscului

Identificarea evenimentelor denotă capacitatea companiei de a detecta evenimentele pozitive și negative, care pot prejudicia sau aduce beneficii companiei. Acest pas afectează realizarea obiectivelor entității. Evenimentele pot fi următoarele:

- ❖ Interne sau externe;
- ❖ Pozitive (oportunități) sau negative (riscuri);
- ❖ Identificare inițială sau identificare continuă.

Evaluarea riscului reprezintă capacitatea companiei de a analiza riscurile, de a înțelege impactul și de a stabili modul în care acestea trebuie gestionate. În practică, din perspectiva probabilității apariției, riscurile, de obicei, sunt clasificate de la „scăzut” – probabilitate foarte mică, la „crescut” – o mare probabilitate, bazată pe așteptările că acele riscuri ar putea să se materializeze.

According to this cycle there are four steps in the process of risk management:

- Step 1. Assessment of risk;
- Step 2. Evaluation of risk;
- Step 3. Management of risk;
- Step 4. Measuring risk's impact.

The first step is to identify or assess the risks, by identifying their source. The sources of the risks can be internal or external to the system. They both can be controlled only up to a certain extent.

After the risks are identified they must be evaluated from the point of view of their potential to be harmful to the company. The potential is calculated taking into account the likelihood of occurrence and the estimated impact. After the evaluation is completed, the risk management plan is development and implemented. It defines the control mechanisms that should be used for the mitigation of risk.

Methods, techniques and steps used in risk management

Event identification is the ability of the company to identify the positive and the negative events which can affect or bring benefits to the company. This step is affecting the achievement of an entity's objectives. The events may be:

- ❖ Internal or External;
- ❖ Positive (opportunities) or Negative (risks);
- ❖ Initial identification or continuous identification.

Risk Assessment is the ability of the company to analyse the risks, to understand the impact and to establish how these should be managed. In practice, from the perspective of their probability to occur, the risks are usually categorized from “low” – very small probability, to “high” – great probability, based on the expectations for the risks to happen.

	Probabilitate/ Probability	Evaluare și descriere/ Assessment and description
Risc crescut/ Traffic Light	> 80% / Greater than 80%	Se așteaptă apariția riscului, care este aproape sigură/ Is expected to occur, almost certain
Mediu/crescut/ Medium/High	între 20% și 80%/ Between 20 and 80%	Risc ce va apărea, existând posibilitatea ca măsurile aplicate să poată sau să nu poată reduce șansele de apariție/ Will probably occur, measures may or may not exist to reduce likelihood
Mediu/ Medium	între 10% și 20%/ Between 10 and 20%	Riscul ar putea apărea, acest lucru este posibil. Există măsuri de reducere a probabilității, dar nu pot fi pe deplin eficiente/ Could occur, this is possible. Measures to reduce likelihood exist, but may not be fully effective
Scăzut/Mediu/ Low/Medium	între 5% și 10% / Between 5 and 10%	Riscul ar putea să apară la un moment dat. Există condiții ca acest lucru să se producă, dar există control și sunt eficiente/ Might occur at some point in time. Conditions do exist for this to occur, but controls exist and are effective
Scăzut/ Low	< 5% / Less than 5%	Riscul poate să apară în situații excepționale. Nicio experiență sau puțin pentru un eșec asemănător/ Rare, may occur in exceptional circumstances. No or little experience for a similar failure

**Figura 2. Probabilitatea de risc pe plan corporativ și operațional/
Figure 2. Probability for Corporate and Operational Plan Risk**
Sursa: elaborată de autor/ Source: elaborated by the author

Impactul riscurilor poate fi, de asemenea, clasificat de la „scăzut” la „ridicat”, în funcție de daunele pe care le pot provoca, în eventualitatea în care acestea se pot întâmpla.

The impact of risks can be also graded from “low” to “high”, depending on the damages they may cause in the event they may happen.

Impact/ Grade of Impact	Descriere/ Description
Ridicat/ High	Pot cauza eșecul în atingerea obiectivelor-cheie. Un impact foarte important asupra obiectivelor organizaționale. Implicații juridice sau de reglementare. Un impact semnificativ asupra reputației/ May cause key objectives to fail. Very significant impact on organizational goals. Legal or regulatory implications. Significant reputational impact.
Mediu/Ridicat/ Medium/High	Efect major. Factorul de risc poate duce la întârzieri semnificative sau la nerealizarea obiectivelor/ Major effect. Risk factor may lead to significant delays or non-achievement of objectives.
Mediu/ Medium	Efect moderat. Factorul de risc poate duce la întârzieri sau la creșterea costurilor/ Moderate effect. Risk factor may lead to delays or increase in cost.
Scăzut/Mediu/ Low/Medium	Impact minor/ Minor impact.
Scăzut/ Low	Impact nesemnificativ, poate duce la o întârziere tolerabilă în atingerea obiectivelor sau la o reducere nesemnificativă a calității / cantității și / sau a creșterii costurilor/ Fairly insignificant, may lead to a tolerable delay in the achievement of objectives or minor reduction in Quality/Quantity and/or cost increase.

**Figura 3. Probabilitatea de risc pe plan corporativ și operațional/
Figure 3. Impact for Corporate and Operational Plan risk**
*Sursa: elaborată de autor în baza sursei [4]/
Source: elaborated by the author based on the source [4]*

Răspunsul în fața apariției riscurilor [4, pag. 6].

Răspunsurile gestionării riscurilor pot fi tratate printr-un mix a cinci acțiuni principale: transferul, tolerarea, tratarea, eliminarea sau valorificarea acestora. **Transferul** – pentru anumite riscuri, cel mai bun răspuns îl poate constitui transferul acestora. Acest lucru se poate face prin asigurarea convențională sau prin sprijinirea unui terț, care-și poate asuma riscul în alt mod.

Tolerarea – capacitatea de a face ceva, astfel, încât anumite riscuri să poată fi limitate sau costul acțiunii să fie disproporționat față de beneficiul potențial dobândit. Acest tip de acțiune este cunoscut și este comun pentru marile riscuri externe. În aceste cazuri, răspunsul poate fi tolerarea, dar riscul trebuie monitorizat, astfel, încât managerii să fie mereu pregătiți să reconsidere acțiunile, dacă acest risc ar prezenta un grad de creștere. Nivelul de toleranță, care determină gradul de risc care poate fi suportat, trebuie să fie stabilit la fiecare nivel și să aibă impact asupra deciziilor ulterioare.

Tratarea – în general, acestei categorii îi aparține un număr mare de riscuri. Scopul acțiunilor de reducere a acestor riscuri nu este neapărat să evite riscul, ci să-l rețină la un nivel acceptabil. Riscul poate fi transferat în susul și în josul lanțului corporativ. Riscurile la nivel înalt ar trebui să treacă la un nivel mai înalt de responsabilitate, pentru a decide asupra unei acțiuni, în timp ce alte riscuri se pot traduce în activități orientate la diminuarea lor. E necesar să se decidă ce criterii vor determina ca riscul să treacă la sistemul de management corporativ.

Eliminarea riscului, se va săvârși, realizând lucrurile în mod diferit, eliminând astfel riscul, acolo, unde este posibil acest lucru.

Exemplul practic pentru răspunsul la așa risc îl constituie cazul garanției pe termen lung pentru un autoturism:

Response to risks [4, p. 6].

Risk management responses can be a mix of five main actions; transfer, tolerate, treat, terminate or take the opportunity. **Transfer** – for some risks, the best response may be to transfer them. This might be done by conventional insurance or by supporting a third party to take the risk in another way.

Tolerate – the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. This course of action is common for large external risks. In these cases, the response may be toleration but the risk should be tracked so managers are ready to reconsider should it start to escalate. Tolerance levels determining how much risk can be taken at each level need to be set and should inform your decisions.

Treat – generally, for this category is specific a greater number of risks. The purpose of taking action to reduce the chance of the risk occurring is not necessarily to obviate the risk, but to contain it to an acceptable level. Risk will be passed up and down the corporate chain. High-level risks may have to pass to a higher level of responsibility to decide on an action, whereas other risks may translate into activities designed to mitigate them. It is necessary to decide what criteria will result in the risk being passed up the corporate management system.

Terminate the risk by doing things differently thus removing the risk where it is feasible to do so.

Practical example for the risk response would be the case of long-term warranty for car:

- Transfer – can be transferred to an insurance company and the company pays only a fix fee;
- Tolerate – take the risk and build an efficient system of service and saving costs;

- Transferul – poate fi transferat unei companii de asigurări, iar compania va plăti doar o taxă fixă;
- Tolerarea riscurilor și construirea unui sistem eficient de servicii și economisirea costurilor;
- Tratatamentul 1 – de transferat numai evenimentele mari (de asigurat numai daune de până la 1.000 euro/ eveniment);
- Tratatamentul 2 – de transferat problemele ce se pot extinde;
- Eliminarea – vânzarea tuturor autoturismelor la încheierea garanției.

Modele de management al riscurilor

Cele mai utilizate modele de gestionare a riscurilor, ce au fost standardizate și utilizate frecvent de către practicieni, la nivel internațional, sunt modelele ISO 31000 și COSO ERM. Acestea nu sunt modele, care încercă să cuantifice sau să evalueze riscul, ci modele pentru guvernarea riscurilor, și anume, modul în care liderii de afaceri ar trebui să abordeze problema riscului.

ISO 31000 [1, p. 3] este un standard acceptat la nivel internațional pentru implementarea principiilor de gestionare a riscurilor. A fost creat, în 2009, de către Organizația Internațională pentru Standardizare, o organizație independentă, non-guvernamentală și cel mai mare dezvoltator, la nivel mondial, de standarde internaționale. Ideea de bază din spatele acestui model constă în faptul că riscurile, care decurg din lipsa ordinii organizaționale, pot fi controlate printr-o mai bună gestionare și guvernare. ISO 31000 oferă un set de principii și linii direcționale generale privind gestionarea riscurilor, un cadru și un proces de gestionare a riscurilor. ISO 31000 intenționează să ajute organizațiile de toate dimensiunile, indiferent de industria în care activează, să crească șansele de a-și atinge obiectivele, să identifice, în mod corect, oportunitățile și amenințările și să aloce eficient

- Treat 1 – transfer only big events (insure only damages up from 1.000 euro/event);
- Treat 2 – transfer epidemic problems;
- Terminate – sell all the cars when warranty is over.

Risk management models

The most commonly used risk management models that have been formalized and frequently used by practitioners, at international level, are ISO 31000 Models and COSO ERM. They are not models that attempt to quantify or assess risk but models for risk-governance, that is, how business leaders should approach the problem of risk.

ISO 31000 [1, p. 3] is an internationally agreed standard for the implementation of risk management principles. It was created in 2009 by the International Organization for Standardization, an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards. The basic idea behind this model is that those risks that arise from lack of organizational order can be controlled through better management and governance. ISO 31000 provides a set of principles and generic guidelines on risk management, a framework and a process for managing risk. ISO 31000 intends to help organizations of all sizes, regardless of the industry they activate in, increase the chances of achieving their objectives, to correctly identify opportunities and threats, and effectively allocate resources for the treatment of risks. The model can be applied to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

ISO 31000 standards are composed of three elements:

- *Risk management process* – assessment and treatment of risks;

resursele pentru tratarea riscurilor. Modelul poate fi aplicat unei game largi de activități, inclusiv strategii și decizii, operații, procese, funcții, proiecte, produse, servicii și active.

Standardul ISO 31000 rezidă în următoarele trei elemente:

- *Procesul de management al riscului* – evaluarea și tratarea riscurilor;
- *Cadrul de management al riscului* – structura ciclului de gestionare a riscurilor în întreaga organizație;
- *Principiile de gestionare a riscurilor* – oferă orientări pentru acțiunile de gestionare a riscurilor.

Procesul standard (prezentat în figura 4) constă din următoarele patru etape:

- *Planificarea și proiectarea cadrului de evaluare a riscurilor* – identificarea, analizarea și evaluarea riscurilor;
- *Implementarea* – tratarea riscurilor;
- *Monitorizarea și revizuirea* – măsurarea rezultatelor și ameliorarea procesului;
- *Îmbunătățirea continuă* – învățarea și raportarea, comunicarea și consultarea.

- *Risk management framework* – risk management cycle structure across the organization;
 - *Risk management principles* – provide guidance for risk management actions.
- The standard process (presented in figure 4)

follows the following four steps:

- *Planning & Design of the risk assessment framework* – identify, analyse and evaluate risks;
- *Implementation* – treatment of risks;
- *Monitor and review* – measuring the results and improving the process;
- *Continuous improvement* – learning and reporting, communication and consultation.

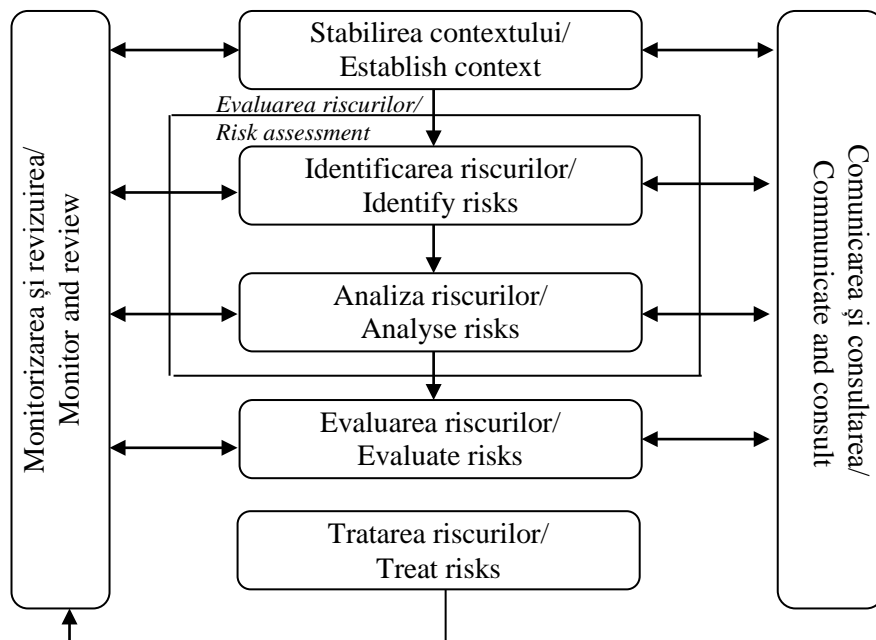


Figura 4. ISO 31000 managementul riscului/ Figure 4. ISO 31000 Risk-management

Sursa: elaborată de autor în baza sursei [1]/

Source: elaborated by the author based on the source [1]

ISO 31000 oferă orientări generale și nu intenționează să promoveze un model uniform de gestionare a riscurilor în cadrul organizațiilor. Proiectarea și punerea în aplicare a planurilor și a cadrelor de gestionare a riscurilor trebuie adaptate, în funcție de diferite aspecte specifice ale fiecărei organizații, la obiectivele, structura, operațiile, procesele, funcțiile și practicile specifice, pe care le utilizează și le promovează.

ISO 31000 oferă, de asemenea, un set de acțiuni care pot fi întreprinse atunci, când sunt abordate riscurile:

- evitarea oricăror activități, care prezintă un risc;
- acceptarea riscului prin desfășurarea activității, care îl implică pentru a-și exercita o oportunitate;
- atenuarea riscului prin eliminarea sursei de risc;
- atenuarea riscului prin schimbarea probabilității sale sau a consecințelor lui;
- împărțirea riscului cu terții.

ISO 31000 este proiectat pentru a se potrivi oricărui tip de organizație, din orice industrie, și conține un set de principii pentru crearea unui cadru de gestionare a riscurilor. Deși se intenționează ca modelul dat să se aplice oricăror riscuri și să fie foarte practic în furnizarea unui ghid eficient pentru gestionarea riscului întreprinderii, acesta nu dispune de instrucțiuni detaliate specifice privind identificarea și gestionarea riscurilor și nu oferă o gestiune completă a riscurilor. De asemenea, în ciuda faptului că este un concept foarte important în managementul riscului, apetitul de risc al unei organizații nu este inclus în cadrul oferit de acest model.

Modelul COSO ERM [5]

În anii 90, (COSO) Comitetul Organizațiilor Sponsor ale Comisiei Treadway a elaborat un model de evaluare a controalelor interne, denumit modelul COSO, care, ulterior, a fost actualizat și definit ca model COSO ERM. Cadrul ERM al COSO definește *Managementul Riscului de Întreprindere* (ERM) drept procesul

ISO 31000 provides generic guidelines and it is not intended to promote a uniform model of risk management across organizations. The design and implementation of risk management plans and frameworks need to be adapted to the varying specific aspects of an organization, its particular objectives, structure, operations, processes, functions and specific practices it uses and promotes.

ISO 31000 also provides a set of actions that can be undertaken when dealing with risks:

- avoiding any activities that present a risk
- accepting the risk by conducting the activity that involves it in order to pursue an opportunity
- risk mitigation by eliminating the source of risk;
- mitigating risk by changing its probability or its consequences;
- dividing the risk with third parties.

ISO 31000 is designed to suit any kind of organization, from any industry, and it contains a set of principles for creating a risk management framework. Even though, it is intended to apply to any kind of risks, and be very practical in providing an effective guide for an enterprise risk management, this model lacks specific detailed instructions on how to identify and manage risks and fails to offer a complete risk management process. Also, despite being a very important concept in risk management, the risk appetite of an organization is not included in the framework provided by this model.

COSO ERM Model [5]

During the 1990's, (COSO) the Committee of Sponsoring Organizations of the Treadway Commission, developed a model for evaluating internal controls, named the COSO model that was later updated and defined as COSO ERM model. COSO's ERM Framework defines *Enterprise Risk Management* (ERM) as a process affected by an entity's management, in setting the strategy across the enterprise, desig-

efectuat de managementul entității, în stabilirea strategiei în întreaga întreprindere. Conceput pentru identificarea eventualelor evenimente care pot afecta entitatea și menține riscul în limitele apetitului pentru risc, să afecteze îndeplinirea obiectivelor entității. Deși a atras critici, cadrul a fost stabilit ca un model, care poate fi utilizat în diferite medii din întreaga lume. Orientarea COSO în modelul ERM este ilustrată sub forma unui cub. COSO a intenționat ca acest cub să ilustreze legăturile dintre obiectivele afișate pe partea superioară și cele opt componente prezentate în față, care sunt necesare pentru atingerea obiectivelor (nivelului de activitate). Cea de-a treia dimensiune reprezintă unitățile organizației și descrie capacitatea modelului de a se concentra asupra unor părți ale organizației, precum și asupra întregului.

ned to identify potential events that may affect the entity, and keep risk within the risk appetite limits, in order not to affect the achievement of entity's objectives. Although it has attracted criticisms, the framework has been established as a model that can be used in different environments worldwide. COSO's guidance in ERM model is illustrated in the form of a cube. COSO intended the cube to illustrate the links between objectives that are shown on the top and the eight components shown on the front, which represent what is needed to achieve the objectives (activity level). The third dimension represents the organization's units, which depicts the model's ability to focus on parts of the organization as well as the whole.

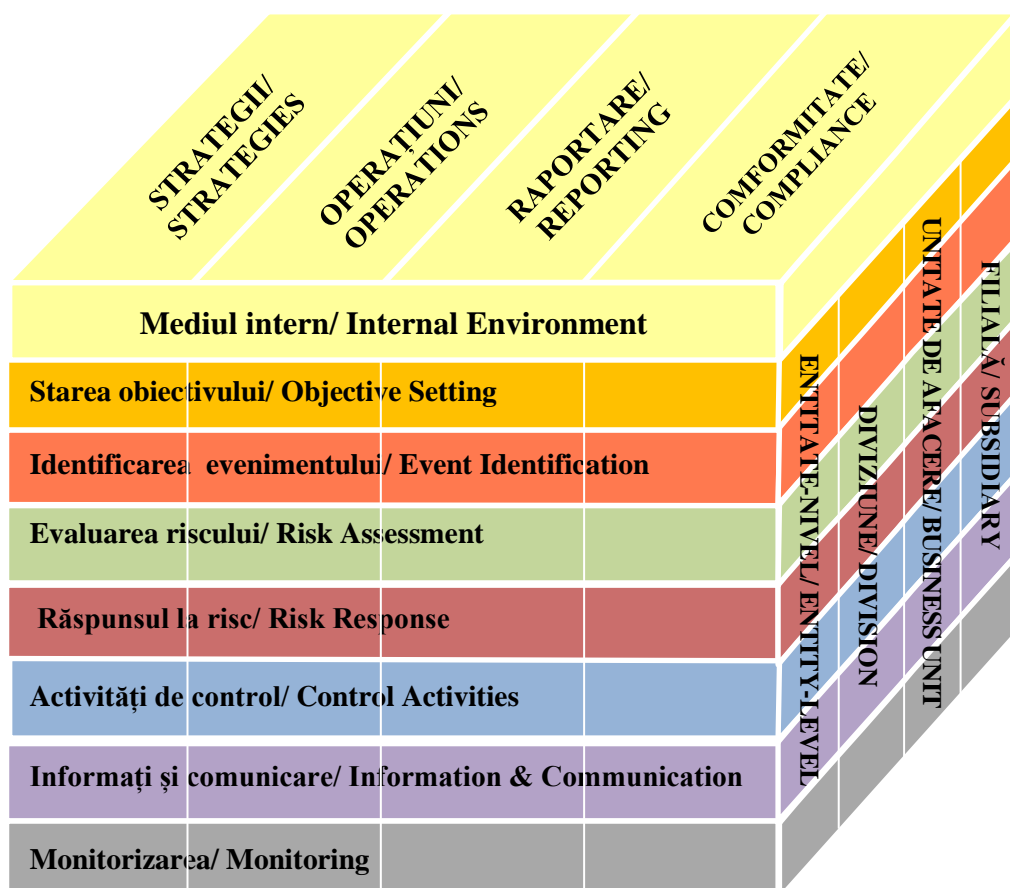


Figura 5. COSO ERM/ Figure 5. COSO ERM
Sursa: elaborată de autor în baza sursei [5]/
Source: elaborated by the author based on the source [5]

Strategia companiei este constituită din patru categorii de obiective:

- obiective strategice – la nivel înalt și orientări strategice;
- operații – modalități eficiente și eficiente de utilizare a resurselor existente;
- raportarea – acuratețea, fiabilitatea, aplicabilitatea rapoartelor elaborate;
- conformitate – respectarea legilor, a procedurilor interne și externe, a reglementărilor.

La nivel organizațional, modelul poate fi aplicat pe patru niveluri diferite: Nivelul entității; Nivelul unității de activitate; Nivelul diviziunii; Nivelul de activitate. La nivelul componentelor, cubul prezintă următoarele elemente:

- Mediul intern – se referă la valorile companiei, la modul în care aceste valori sunt privite și abordate de angajați, în mediul de integritate, în care acționează;
- Stabilirea obiectivelor – cum sunt determinate obiectivele pentru a sprijini strategia entității;
- Identificarea evenimentului – capacitatea companiei de a identifica evenimentele pozitive și negative, care pot afecta sau aduce beneficii companiei;
- Evaluarea riscului – capacitatea companiei de a analiza riscurile, de a înțelege impactul și de a stabili modul în care acestea trebuie gestionate;
- Răspunsul la risc – în conformitate cu strategia entității, în ceea ce privește riscul și atitudinea față de aceasta, trebuie analizată;
- Activitățile de control – capacitatea, activitățile și instrumentele unei companii de a se asigura că, în general, compania urmărește setul de strategii, obiectivele, obiectivele și deciziile luate;

The company's strategy stands on four categories of objectives:

- strategic objectives – high-level targets and strategic guidelines;
- operations – effective and efficient ways of using the existing resources;
- reporting – accuracy, reliability, applicability of the reports developed;
- compliance – compliance with laws, internal and external procedures, regulations.

On the organizational level, the model can be applied on four different levels: Entity level; Business unit level; Division level; Activity level. On the component level, the cube presents following elements:

- Internal Environment – refers to the values of the company, how are these values viewed and addressed by the employees, the integrity environment in which they operate;
- Objective Setting – how are the objectives set in order to support the entity's strategy;
- Event Identification – the ability of the company to identify the positive and the negative events which can affect or bring benefits to the company;
- Risk Assessment – the ability of the company to analyse the risks, to understand the impact and to establish how these should be managed;
- Risk Response – according to the entity's strategy in relation to risk and the attitude towards this must be analysed;
- Control Activities – the ability, activities and tools of a company to make sure that overall the company is following the strategy set, objectives, targets and decisions taken;

- Informarea și comunicarea – din punctul de vedere al acurateții și al timpului, modalitățile de transmitere a informațiilor în cadrul unei companii este un punct crucial de analizat;
- Monitorizarea – capacitatea companiei de a urmări și de a fi permanent conștientă de rezultatele, numerele și cifrele actualizate.

Aceste componente contribuie la stabilirea bazei pentru controlul intern, în cadrul companiei, prin intermediul conducerii direcționate, al valorilor comune și al unei culturi, care accentuează responsabilitatea pentru control. Diferitele riscuri, cu care se confruntă compania, sunt identificate și evaluate la toate nivelurile și în cadrul tuturor funcțiilor din cadrul organizației. Activitățile de control și alte mecanisme sunt concepute pentru abordarea și atenuarea riscurilor semnificative într-o manieră proactivă. Informațiile esențiale pentru identificarea riscurilor și îndeplinirea obiectivelor de afaceri sunt comunicate prin intermediul canalelor stabilite, în sus, în jos și în întreaga companie. Întregul sistem de control intern este monitorizat în mod continuu și problemele sunt abordate în timp util.

Scopul principal al acestui cadru a fost, pe de o parte, prevenirea riscului, prin detectarea acestuia, mai întâi prin analiza controlului intern, apoi prin abordarea, în continuare, a riscului la fiecare nivel diferit, acolo unde apare.

Modelul COSO ERM a oferit fundațiilor posibilitatea să evalueze riscurile și să le gestioneze mai eficient. Este un instrument mai practic, care poate fi folosit de către manageri pentru a evita posibilele crize. Modelul sus-menționat construiește concept-cheie, fundamentale pentru definirea unui sistem de management al riscului organizațional, oferind o bază importantă pentru aplicare, în cadrul organizațiilor, a direcțiilor și sectoarelor economice.

- Information and Communication – from accuracy point of view and time wise, the ways of transmitting information within a company it's a crucial point to be analysed;
- Monitoring – the ability of the company to follow up and permanently be aware of the updated results, numbers and figures.

These components work to establish the foundation for internal control within the company through directed leadership, shared values and a culture that emphasizes accountability for control. The various risks facing the company are identified and assessed at all levels and within all functions in the organization. Control activities and other mechanisms are designed to address and mitigate the significant risks in a proactive manner. Information critical to identifying risks and meeting business objectives is communicated through established channels up, down and across the company. The entire system of internal control is monitored continuously and problems are addressed in due time.

The main purpose of this framework was on one side to prevent the risk by detecting them first through internal control analysis and further by addressing the risk at each different level where it arises.

The COSO ERM model has provided a foundation for organizations to assess the risks and then manage them more efficiently. It is a more practical tool that can be used by managers in order to avoid possible crises. It builds key concepts, fundamental for defining an organizational risk management system, providing a basis for application across organizations, industries, and sectors.

The only available tools in practice, used by companies in order to prevent crises, are the risk management models. The most common used ones are ISO 31000 and COSO ERM.

Singurele instrumente disponibile în practică, utilizate de companii pentru prevenirea crizelor, sunt modelele de gestionare a riscurilor. Cele mai des folosite sunt ISO 31000 și COSO ERM. Aceste modele sunt în măsură să ofere doar o orientare sau o hartă generală, cu ajutorul căreia managerii pot urmări și menține organizațiile lor în condiții de siguranță în cazul riscurilor și crizelor, care pot surveni din cauză că acestea sunt, mai degrabă, modele teoretice, care nu se bazează pe un algoritm matematic.

Concluzii

Procesul de identificare, evaluare și atenuare a potențialelor amenințări, ca parte a procesului de management al crizelor, se numește prevenirea crizelor. Implementat în cadrul unei organizații ca un proces continuu de prevenire a crizelor sau gestionare a riscurilor, va diminua considerabil probabilitatea ca organizația să se confrunte cu o criză. Expunerea la crize nu va scădea la zero, deoarece există întotdeauna un anumit procent de riscuri care nu pot fi niciodată eliminate complet, dar șansele de a evita o criză și de a se redresa după o criză vor fi mult mai mari, atunci, când organizația adoptă măsuri de prevenire a crizelor/ abordarea managementului riscului.

În general, managementul riscului și gestionarea crizelor nu concurează ca practici în cadrul unei organizații, ci conlucrează pentru același rezultat, ceea ce sporește capacitatea unei organizații de a face față, în modul cel mai eficient, oricărei posibile amenințări care ar putea pune în pericol funcționalitatea sau chiar existența sa.

Există o legătură puternică între practicile de gestionare a riscurilor și de gestionare a crizelor. Atât managementul crizelor, cât și managementul riscului fac parte din domeniul general al managementului organizațional și ambele se ocupă de amenințările care afectează buna funcționare a sistemelor organizației și bunăstarea indivizilor săi.

These models are only able to provide a guideline or a general map that managers can follow in their attempt to keep their organizations safe from risks and crises, which leaves a lot of room for subjectivity and human error due to the fact that they are rather theoretical models, not based on a mathematic algorithm.

Conclusions

The process of identifying, assessing and mitigating potential threats as part of the larger crisis management process is called crisis prevention. Implemented within an organization as a continuous process, crisis prevention or risk management will diminish considerably the probability for the organization to face a crisis. The exposure to crises will not decrease to zero, as there is always a certain percentage of risks that can never be eliminated, but the chances of avoiding a crisis and recovering after a crisis will be much higher when the organization is adopting a crisis prevention/risk management approach.

In general, risk management and crisis management are not competing as practices within an organization; rather, they are working together for the same outcome, which is increasing the capacity of an organization to cope in the most efficient way with any possible threat that might put in danger its functionality or even its existence.

There is a strong connection between the risk management and crisis management practices. Both, crisis management and risk management are part of the general domain of organizational management and they both deal with threats that impact the well running of the organization's systems and the wellbeing of its individuals.

Bibliografie/Bibliography:

1. AIRMIC, Alarm, IRM, „*A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*”, 2010. ISBN 978-0-749459420.
2. GUNNING, J. G. and J. I. C. HANNA. „The Application of Risk Management Principles to Crisis Management Construction”, Akintoye, A (Ed.) (2001) *17th Annual ARCOM Conference, 5-7 September, University of Salford*. Association of Researchers in Construction Management, vol. 1, page 815. ISBN 978-0-9552390-9-0.
3. KNIGHT, Frank. (1964) „*Risk, Uncertainty and Profit*”, Augustus M. Kelley, New York, page 20.
4. Her Majesty's Treasury, Risk management assessment framework: a tool for departments, 2009, UK Government, Office of Public Sector Information.
5. http://www.coso.org/documents/coso_erm_executivesummary.pdf