ASPECTS OF RISK MANAGEMENT INTRODUCTION IN SMALL AND MEDIUM ENTERPRISES

Luise Zeininger
luise.zeininger@gmail.com
The Bucharest Academy of Economic Studies, Bucharest, Romania
Sabina Irimie
sabina.irimie@gmail.com
University of Petroşani, Romania

The main objective of this paper is to provide a perspective on the main characteristics of approaching Risk Management by micro, small and medium enterprises' top management based on both European Union regulatory documents and also on ISO standards - mainly ISO 31000:2009 Risk management - Principles and guidelines. The paper aims to present some aspects of the main approaches on what is the role of Risk Management within a modern organisation and how is Risk Management introduction tied to organisational structure and culture, to top management risk aversion.

Keywords: management, business objectives, risk management,

JEL Code: L21, M10

1. Introduction

The world is spinning faster and businesses and regulators all together, operate and work in a new, so called "risk environment" that is increasingly complex. After the financial crisis of 2008, the "risk environment" became our "risk normality" that we strive to cope with on a daily basis. Organisations of all types and sizes are facing a range of risks affecting the achievement of their objectives. While risk is commonly regarded as negative, risk management is as much about exploiting potential opportunities as preventing potential problems.

Many observers attribute the 2008 collapse to financially risky behavior of a magnitude never before experienced exposing the U.S. credit markets of the time as a financial house of cards with a faulty foundation built by unethical behavior in the financial markets:

1. Lenders gave home mortgages without prudent risk management to underqualified home buyers, starting the so-called subprime mortgage crisis.
2. Home prices started to decline simultaneously as many of the unqualified subprime mortgage holders had to begin paying larger monthly payments. They could not refinance at lower interest rates as rates rose after the 9/11 attacks.
3. Financial institutions guaranteeing the mortgage loans did not have the appropriate backing to sustain the large number of defaults. These firms thus lost ground, including one of the largest global insurers, AIG (American International Group).
4. Many large global financial institutions became insolvent, bringing the whole financial world to the brink of collapse and halting the credit markets.
5. Individuals and institutions such as banks lost confidence in the ability of other parties to repay loans, causing credit to freeze up.
6. Governments had to get into the action and bail many of these institutions out as a last resort. This unfroze the credit mechanism that propels economic activity by enabling lenders to lend again.

As we can see, a basic lack of risk management (and regulators' lack of attention or inability to control these overt failures) lay at the heart of the global credit crisis. This crisis started with a lack of improperly underwritten mortgages and excessive debt. Companies depend on loans and lines of credit to conduct their routine business. If such credit lines dry up, production slows down and brings the global economy to the brink of deep recession—or even depression. The snowballing effect of this failure to manage the risk has been profound, indeed.

Following those events and due to its repercussions on European Union members such as Greece, Spain, Portugal, Regulators all over European Union strived to find ways and means to help businesses to be successful despite the fast spinning of the business environment. Following this

approach Directive 34 was developed in 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.

The non financial report that is introduced EU/34/2013 states that: "in reporting on internal control and risk management systems, the corporate governance statement shall refer to the main features of the internal controls and risk management systems for the undertakings included in the consolidation, taken as a whole"(art 29, alin2b).

Thus, it is incumbent for Romanian Parliament to develop the legal framework up to 20.07.2015 since the requirements should apply starting with the financial year beginning as of 01.01.2016 or anytime later.

On the other hand the standard ISO 31000:2009, *Risk management – Principles and guidelines*, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance.

Having regulatory requirements on one hand and ISO instruments on the other how would better approach Risk Management a small enterprise? If "any organisation exists to achieve certain objectives that draw from its activities and beyond this objectives there is no organisation as there are the objectives that represent the reason to be of the organisation (Nicolescu, Verboncu and Profiroiu, 2011, p. 15), how would it even define risk and where would it look to find its elements? This is the aim of this paper to discuss and depict.

First part of the paper is dedicated to introducing general key-concepts. Second part is looking at risk management approaches and the third part is all about stages and obstacles in implementing an efficient and effective Risk Management System (RMS) within organisation.

2. Key-concepts on risk and managing risk

What is risk? It is known that Eskimos have a dozen or so of words to name or describe snow. Likewise, professional people who study risk use several words to designate what others intuitively and popularly know simply as "risk." Professionals note several different ideas for risk, depending on the particular aspect of the "consequences of uncertainty" that they wish to consider. Using different terminology to describe different aspects of risk allows risk professionals to reduce any confusion that might arise as they discuss risks.

There are several meaningins and definitions. Dumitraşcu (2012) identified over 300 bibliographic entries on risk management and Aven (2010) has no less than 20 risk definitions, rather likely to understood for such a inter- and multidisciplinary subject. According to ISO PAS 28000 risk is the "likelihood of a security threat materializing and the consequences"(definition 3.1, pag. 3). According to ISO guide 73:2009 risk is "the effect of uncertainty over objectives" (definition 1.1.) and this is also the definition used also by ISO 31000:2009 and by the Romanian legislation such as the order 946/2005 of Public Finance Ministry regarding the approval of the Internal/managerial Code of control - including the internal control standards for public entities - republished in 2012. Order 946/2005 defines risk as follows: "the events that might affect objectives achievement are risks that should be identified".

Risk is also defined by various authors as being a situation (Iloiu, 2005), an event (Dumitraşcu, 2012), that did not occured yet, but may occure in the future, and in case it occurs it threats, realistic or potential, the achievement of the desired results; risk is the uncertainty in achieving the desired results (Lupton, 1999a), (Lupton, 1999b), (Toma, Chitită & Şarpe, 2012). There are various definitions used by Romanian Dictionaries, for example: risk is a "possible threat" (Canarache and Breban, 1974) and as "the possibility to be in danger, to come accross trouble, having to face a loss or damage; possible threat" (DEX 2009)

Till not too long ago, financial crisis from 2008 playing a major role in the shift, risks were connected solely with Health & Safety occasionally including fire prevention. Fox (1999) considers that risk is the antagonist of safety but also that it offers opportunities. The same opinion is expressed by Baranoff, Brockett & Kahane, 2015.

Since 2008 the management risk perception within small and medium enterprises top managers shifted form a narrow view of internal risks related to health & safety and financial risk of rate exchange and late payments to a broader understanding so it includes mostly external risks such as: natural risks, political risks, legal risks, socio-cultural risks in addition to the internal ones: financial risk, operational risk, management risks to name just some of the most important ones.

Natural risks- are related to all natural hazards that a business operations may encounter. It will not only affect agrarian businesses but almost any enterprise on the food chain, construction enterprises with a cascade effect on their suppliers. Due to the natural factors influences that could cause either rises or decreases in productivity businesses have added the environmental risk on their agenda. Environmental risks could also be included here when considering them related to natural elements such as water, air, soil, waste.

Political risk- are related to changes of Governement strategies and actions at both European Union level and national level.

Legal risks- are related to changes in the legal framework of the environement that the enterprise is active.

Socio-cultural risks - are related to social environment, labour force, the culture of the enterprise and its strategies, politics and procedures in place.

Trading risks - are related to the supply and sale operations on the internal and external market, the most important being: the price risk, the transport risk and the storage risk, the sale risk *(Iancu and Mondoca, 2006)*

Financial risks - are related to capital usage and availability and may cover several aspects of managing a business: difficulty of accessing credits, exchange rate risks, inflation risk, interest rate risks, investment risks.

Operational risks- are related to technological risk of an enterprise and even this types of risks are easier to predict their cost might be higher because of their specificity; for example it is easy to predict the annual revision of a production line and the direct cost associated: spare parts, duration, production hours loss but the risk may came from a delay in receiving a specific spare part that will unleash an unexpected increase of all sort of effects: delay in production, delay in fulfilling a due-date order, penalties because of that and so on. Operationl risks would also include e-risks related to: security information breach, on-line activities, on-line communications, data loss.

Management risks - are related to both the management as system and as humans. Management risks could be about an outdated management system in place but also about poor management capabilities of the top management team in place.

Pure risks - the risks that features some chance of loss and no chance of gain (e.g. fire risk, flood risk, etc.).

Speculative risks - the risks that feature a chance to either gain or lose (including investment risk, reputational risk, strategic risk, etc.)

Risk tolerance - the quantity of risk that an organisation is able to tolerate or is willing to be exposed to at a specific moment in time/ timeframe.

Inherent risk - risk exposure before any action is taken

Residual risk - the risk that remains after its treatment

Risk management - is a central part of any organisation's strategic management being defined as a a methodically coordinated set of activities in order to direct and control organisational risk (definition 2.2, p. 9), (Baranoff, Brockett & Kahane, 2015), (Jorion, 2010), (Suciu & Trifan, 2014). In other words risk management is the process whereby organisations methodically address the risks related to their activities with the goal of achieving their objectives.

Some of the above mentioned risks are at the border line between internal and external business environment demanding an integrated approach related to organisation's objectives.

3. Risk management approaches

ISO 31000:2009 is a generic risk management standard that provides the framework, by providing the principles and and guidelines, to develop a RMS within organisation no matter what size it is or what it does. It can be used by both public and private organisations and also by groups, associations, and enterprises of all types. It is not specific to any sector or industry and can be applied to any type of risk. ISO 31000 can be applied to the achievement of any and all types of objectives at all levels and areas within an organisation. It can be used at a strategic or organisational level to help make decisions and can be applied to all types of activities. It can be used to help manage processes, projects, programs, operations, products, services and assets.

When taking the ISO 31000:2009 route in approaching risks management team and the risk management team should start by approaching its principles as defined by the standard:
a) *Risk management creates value* - risk management creates and protects value by helping managers to achieve their organisation's objectives and improve its performance;
b) *Risk management is an integral part of organizational processes*. Risk management is part of every process at every level being the responsibility of every manager;
c) *Risk management is part of decision making*. Risk management is used to make informed choices and prioritise actions;
d) *Risk management explicitly addresses uncertainty.* Risk management is used to identify and define the nature and type of uncertainties that an organisation would deal with and to decide what management could do to address those;
e) *Risk management is systematic, structured and timely*;
f) *Risk management is based on the best available information*. The inputs to the process of managing risk should be based on information sources such as experience, feedback, observation, forecasts and expert judgement. However, decision makers should be informed of and should take into account any limitations of the data or modelling used or the possibility of divergence among experts;
g) *Risk management is tailored*. Should take into account both the organization's external and internal context and its risk profile;
h) *Risk management takes human and cultural factors into account*;
i) *Risk management is transparent and inclusive*;
j) *Risk management is dynamic, iterative and responsive to change*. As internal and external events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore an organisation should ensure that risk management continually senses and responds to change;
k) *Risk management facilitates continual improvement and enhancement of the organisation*.

By applying in a structured, systematic way the above principles and the framework developed by ISO 31000 any organisation would be able to:

- Increase the likelihood of achieving objectives;
- Encourage proactive management;
- Be aware of the need to identify and treat risk throughout the organisation;
- Improve the identification of opportunities and threats;
- Comply with relevant legal and regulatory national requirements and also with international norms;
- Improve financial reporting;
- Improve stakeholder confidence and trust;
- Establish a reliable basis for decision making and planning;
- Improve controls;
- Effectively allocate and use resources for risk treatment;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance, environmental protection, data protection;
- Improve loss prevention and incident management;
- Minimize losses;
- Improve organisational learning & development.

Risk assessment is part of risk management which provides a structured process for organisations to identify how objectives may be affected. As a tool, risk assessment is used to analyse risk in terms of both consequences and their probabilities, before the organisation decides on further treatment, if any required.

Any organisation taking this road any manager assessing risk would come across following questions:

- What could happen and why?
- What would be the consequences of that happening?
- What is the probability of their future occurrence?
- Are there any factors that would reduce probability and/or consequences of the risk?

Good news is that all the organisations and all the managers facing those questions would find handy to use ISO 31000 and also a third standard, ISO/IEC 31010:2009, *Risk management – Risk assessment techniques* that has been developed jointly by ISO and its partner IEC (International Electrotechnical Commission).The standard provides a basis for management to decide about the most

appropriate approach to treat particular risks of their organisation and select between options. ISO/IEC 31010 will assist organizations in implementing the risk management principles and guidelines provided in ISO 31000.

Having in mind the soon to be implemented EU regulation on non-financial-reporting implementation of a RMS would help prepare any organisation to face with better chances business environment changes and achieve its compliance objective. according to EU regulation European undertakings are classified into: micro-undertakings, small, medium and large undertakings based on three criteria: average number of employees during financial year, net turnover and balance sheet total, providing that at least two out of three do not exceed the established limits. (art. 3/ UE / 34/2013)

As stated in the introduction of the EU/34/2013 while large undertakings and "groups are required to prepare extensive financial reports including management reports small undertakings and small groups should be exempt from the obligation to prepare consolidated financial statements as the users of small undertakings' financial statements do not have sophisticated information needs and it can be costly to prepare consolidated financial statements in addition to the annual financial statements of the parent and subsidiary undertakings. Member States should be able to exempt medium-sized groups from the obligation to prepare consolidated financial statements on the same cost/benefit grounds unless any of the affiliated undertakings is a public-interest entity"(paragraph 33, introduction).

4. Stages and obstacles during implementation

The main temporal stages of implemneting EU regulation on macroeconomical level and their objectives are represented in figure 1.

On microeconomic scale, following the strategic decision to implement a RMS, based on risk management principles and ISO 31000:2009 requirements, top managers might just follow the Plan-Do-Check-Act (PDCA) iterative four-step management method used by businesses for the control and continuous improvement of processes and products, also known as the Deming circle/cycle/wheel, especially those that already have a Quality management systems implemented. The PDCA model 4 steps are:

- **PLAN**: establish the risk management policy, objectives, targets, processess and procedures relevant for risk management; establish responsabilities; set authorities; allocate resources; risk identification; analyse and assess risk; develop instruments to maintain records;
- **DO**: implement in a systematic and structured way the elements of step PLAN; could it be controled?
- **CHECK**: monitor and measure step DO and PLAN by monitoring and measuring processess against the set objectives and requirements; is the system efficient? is it effective? audit and report;
- **ACT:** based on reports from step CHECK set corrective/preventive actions in order to ensure continuous improvement of both system and organisational performance.

The obstacles might arise virtually from any step, proccess, action, member of the risk management team. Fear to change, unwillingness to take responsibility, lack of capabilities, misunderstanding of risk, lack of resources, poor communication each or any ot it creates obstacles and delays.

An important element of risk management implementation is communication, both external with impact on how the company is perceived by competition and internal with impact on how risk is dealt with. minitoring, assesing, analysing risk all need to be communicated over several layers within company. Risk communication is usually done via periodical risk reports that would tackle financial aspects such as: risk control measures costs, potential losses costs, insurance costs, potential penalties and operational aspects such as: risk breakdown, control instruments, inherent risk, residual risk (both with detailed description of: probability, impact and exposure), responsibilities, deadlines, risk evolution during monitored period, other pertinent observations made bt risk team members.

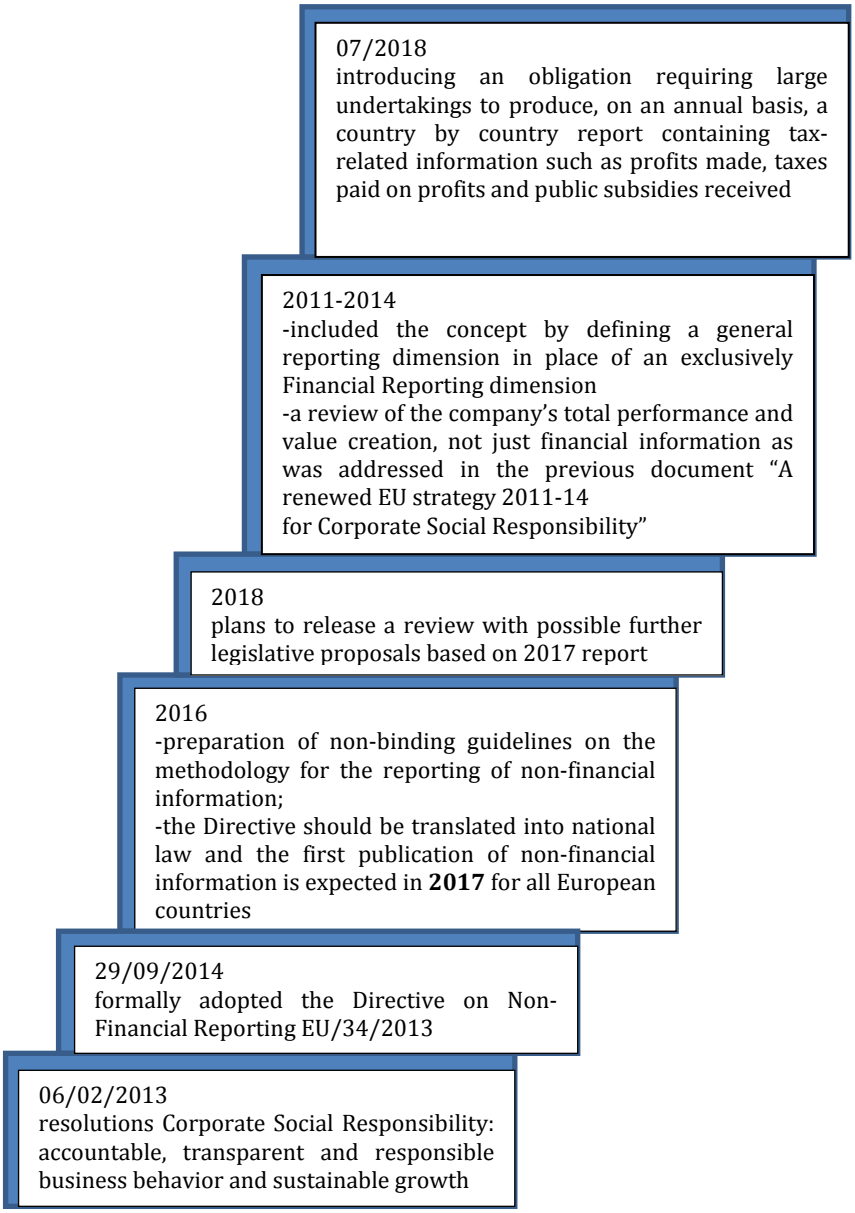

Figure 1 Temporal stages and objectives of EU regulation implementation
Source: Adapted from ECIIA, 2015, pp.5-6

Another approach, endorsed by the Federation of European Risk Management Associations (FERMA) is based on a 3-steps approach that sets-up 3 defence levels - operational, control and internal audit- in pursuing the organisation protection of risks and their effects.

First line of defence, at the operational level consists of the top management team, that is considered to be ultimately responsible for the management of risks and for the internal controls. They are also to be held accountable since they establish the overall risk appetite and the philosophy of risk taking of the company.

Second line of defence, at the control level is about monitoring and implementation of the effective risk management actions decided by the first level. A systematic and systemic approach brings together in this second line the support functions that will work to deliver a risk profile for the whole company.

"Third line is the internal audit. Seen as a management tool as it is recommended by all management systems intrenal audit aims to provide assurence on organisation's effectiveness in assesing and managing its risks and related internal control systems, including the manner in which the 1st ad 2nd line operate" (FERMA / ECIIA, p. 10). Internal audit should not be confused with

financial control nor with quality control as it is neither, though it might include both and also should ensure that the professional requirements for independence and objectivity are not breached. The role of Internal Audit is likely to differ from one organisation to another. In practice, Internal Audit's role may include some or all of the following:

- auditing the risk management processes across an organisation;
- auditing the significant risks, as identified by management;
- providing assurance of an effective management of risk;
- providing active support in improving the overall risk management process;
- facilitating risk identification/assessment;
- educating line staff in risk management and internal control;
- coordinating risk reporting to the top management, audit committee etc.

The way any organisation will arrange its defence lines depends entirely on the maturity, resources and staffing of the second and third line.

The obstacles might be, for this model, a lack of a clear at up of the organisation's risk management policy, since it is the policy that should set out the organisation's approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the whole organisation and last but not least it should refer to any legal requirements for policy statements e.g. for Health and Safety.

Other obstacles could be the misuse of the tools and techniques attached to the risk management process to be effective the risk management process requires: commitment of the top management team; clear assignment of responsibilities within the organisation; transparent allocation of appropriate resources for training and the development of an enhanced risk awareness by all stakeholders.

In all types of undertaking, there is the potential for events that constitute opportunities for benefit (upside), threats to success (downside) or an increased degree of uncertainty.

Also a 3 levels approach is the one that draws on how risks could impact an organisation from the time point of view. Risks can impact an organisation in the short, medium and long term. These risks are related to operations, tactics and strategy, respectively. Operations are the daily routine including all the activities of the organisations. Short term risks are related to operations because their effects are associated with short term lenghts of their effects. For example a daily routine that involves saving data into a computer might be affected by the risk of malfunction if the mouse will not work properly; a flat tyre on one of the cars is also something that impacts only on short term an organisation. These are however risks that could be quickly and with low costs avoided.

Tactical risks are typically associated with projects or product developments. A project may be linked to an initiative reflecting the tactics by which strategy will be implemented. It involves a time period, maybe months or a year, specific resources and objectives achievement. The risks associated with a project running on an organisation would affect it on medium term and it would affect only a part of its operations. So, if, for example a computer would crush following a change of software it would nevertheless affect the project longer than the mouse malfunction but essentially it would not stop the whole organisation.

Strategy sets out the long-term vision, setting the aims of the organisation, and the strategic planning horizon for an organisational strategy will typically be 3, 5 or more years, sometimes as many as 7 or 10. At strategic level risks could impact the firm on long term; a wrong decision on buying hardware or a car fleet aquisition would impact the organisation for several years. Risk management at this level, should be a continuous process that supports the development and implementation of the strategy of an organisation, addressing methodically all of the operations of the businesses.

Risk management should be integrated into the culture of an organisation and in order to achieve that top management involvement is needed as it is top managers that could lead and commit to such long term high level actions. Top management could also translate risk strategy into tactical and operational objectives, and assign risk management responsibilities throughout the organisation, promoting operational efficiency at all levels.

Risk aware top management would lead to a risk aware culture within organisation, ensured by establishing an appropriate risk architecture, strategy and protocols.

A even further interpretation of the 3-levels model is applied on promoted by the European Confederation of Institutes of Internal Auditing (ECIIA) that suggests key-roles of each function in the reporting.

The background of its content is set by the existing regulations either on national level either EU requirements that in order to comply with their corporate social responsibilities, companies should

have in place a process to integrate social, environmental, ethical, human rights and consumer concerns into their business operations and core culture through long-term strategy. For that, top management, should work closely with stakeholders aiming to:

- maximising the creation of value for owners, all stakeholders categories and society at large;
- identify, prevent and mitigate possible adverse impact from operations risks.

<table>
<tr><td></td><td colspan="2">Governing Body/ Audit Committee</td><td rowspan="5">External audit</td><td rowspan="5">Regulator</td></tr>
<tr><td colspan="2">Top Management</td><td></td></tr>
<tr><td>1st line of defence</td><td>2nd line of defence</td><td>3rd line of defence</td></tr>
<tr><td>Management controls</td><td>Risk management</td><td>Internal Audit</td></tr>
<tr><td>Internal control measures</td><td>Financial control</td><td></td></tr>
<tr><td></td><td>Compliance</td><td></td></tr>
</table>

Figure 2: The 3-lines defence model
Source: ECIIA, 2015, p.8

In the first line of defence one founds operational management; in this interpretation operational management has ownership, responsibility and it is accountable for non-financial reporting.

The second line of defence brings on stage risk management together with compliance and financial control. In this line could also be found other support functions that would facilitate and monitor the implementation of an effective non-financial reporting process by operational management acting in the 1st line and assist them in reporting relevant information both upwards and downwards within the organisation.

The third line of defence is dedicated to the internal audit function. Internal auditors provides, based on the ethical professional requirements of independence and objectivity, independent assurance to the organisation's top management on audited issues. Regarding the non-financial reporting process and disclosures specifically, internal audit may provide assurance that the risks are being effectively mitigated based on analysis and actions taken and that suitable controls to keep them on acceptable levels have been implemented.

Managers of small and medium enterprises might also inspire their risk management approach form the public entities legislation. Public entities have to develop and implement an internal control system based on specific requirements documented by OMF 946/2005. The control system is associated with its wider understanding, the one of a managerial function and not its narrow one, as minimal check activity/process. Using its control function management of any type of entity may follow up on whether objectives were achieved as planned, would analyse the causes of any deviation and would implement corrective and preventive actions. Does the iteration sounds familiar? Well, it's just another PDCA approach.

Also of importance in using this piece of legislation as benchmark is their definition for the objectives. Objectives are important since risk is related by not-reaching them. Hence well defined objectives will help better define risk and therefore monitor it with better. Recommendation is that objectives should be SMART (specific, measurable, achievable, relevant and time-bound) (Doran, 1981).

Management of a public entity has the obligation to identify risks and implement measures that would maintain risks within acceptable limits. It is recommended that a balance is maintained between acceptable level of risks and the costs related to the actions that would keep risks at those levels.

"Risk communication within organisation's structure might face various challenges and specific obstacles. These would result because many risk management related concepts are complex and hence difficult to explain and understand. understanding difficulties are also enhanced by the non-specialists receivers of the message. Moreover understanding risk management problematics would require technical knowledge from a range of connected domains.

Another type of difficulties results form teh fact that non-specialists underestimate the meaningfulness of risk management. This is way, risk manager should explaine not only risk consequences and prevention methods but also to underline the importance for the entire organisation of risk management and the positive outcome of implementing a risk management policy. It is only this

way that chances would be that, in the future, the top managers will integrate the risk management vision in their daily routine." (Anastasiei, B., 2011, p.9)

5. Conclusions

Risk itself is neutral - it is important to bear this in mind whenever managing risk. Whether its positive or negative effects affects us and/or our businesses it is manageable. Businesses could make use of the fast spinning of change and find new markets or get burried under the burden of regulations, taxes, compliance costs etc.

Managing risks get, in the end, to 5 possible actions:

1. *Avoid risk.* Avoiding risk as deliberate management action is an option when risks cannot be influenced by an entity. It should take into consideration the limitation such option would set and also the possible opportunities loss.
2. *Retain risk*. Risk retention also as a deliberate management decision means that no further action will be taken to respond to it. The level of risk where management draws the line is a strategic management decision. Risk retention due to failure to identify risk should not be tolerated.
3. *Modify risk*. Risk modification is a management tool designed to make use of potential opportunities and minimise threats associated with certain actions.
4. *Transfer risk*. Risk transfer also known as risk sharing is a usefull managerial tool. No risk could be 100% transferred but incurance, outsourcing, partnerships might limit the exposure. The downside is that will also limit the profitability.
5. *Seek risk*. Actively seeking risks with potential desirable consequences may enhance the attractivity of a specific project/activity.

Some of these actions would just replace a risk with another, some will limit the exposure at the cost of loosing profit or opportunities. In the end it's all about how much risk can the management team take as they have a major influence on risk acceptance level of the organisations. Management team just have to balance the cost of risk control versus the costs of risks so that businesses they run are as safe and profitable as possible in the open-wide business world. That's what businesses are for. Just like William G.T. Shedd used to say "A ship is safe in harbour, but that's not what ships are for."

References:

1. *Anastasiei, B., Aspects of Risk Management in an Organisation, Risk Theory and applications, Nr.1, 2011, pp.4-9*
2. *Aven T., Misconceptions of Risk, John Wiley & Sons Ltd., West Sussex, UK, 2010.*
3. *Baranoff E., Brockett P.L., & Kahane Y., Risk Management for Enterprises and Individuals, v. 1.0, available at http://catalog.flatworldknowledge.com, accessed in March 31 2015*
4. *Canarache A., Breban V., Small Dictionary of Romanian Language, Editura Ştiintifică, Bucharest, 1974*
5. *DEX '09 (2009), available at http://dexonline.ro/definitie/risc/paradigma, accessed in March 31 2015*
6. *Doran G. T., There's a S.M.A.R.T. way to write management's goals and objectives, Management Review (AMA FORUM) 70 (11), 1981, pp. 35–36*
7. *Dumitraşcu D., Risk and its managerial components in organisations businesses, PhD Thesis Summary, "Lucian Blaga" University, Economical Studies Faculty, Sibiu, 2012, available at doctorate.ulbsibiu.ro/obj/documents/Rezumat_lb.rom-dumitrascu.pdf, accessed in March 20 2015*
8. *ECIIA, Enhancing Governance through internal audit (Non-Financial Reporting: Building trust with internal audit), 2015, available at http://www.eciia.eu/wp-content/uploads/2015/04/ECCIA_Brochure_Trust_2015_final.pdf, accessed in April 1 2015*
9. *European Council, Seventh Council Directive 83/349/EEC of 13 June 1983 based on the Article 54 (3) (g) of the Treaty on consolidated accounts*
10. *European Council, Fourth Council Directive 78/660/EEC of 25 July 1978 based on Article 54 (3) (g) of the Treaty on the annual accounts of certain types of companies*
11. *European Parliament and European Council, Directive 2013/34/EU of the of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC*
12. *European Parliament and European Council, Directive 2006/43/EU - Statutory Audit Directive*
13. *FERMA/ECIIA Guidance for Boards and Audit & Risk Committees Brochure v8, available at http://www.belrim.com/app/uploads/2014/12/ECIIA_FERMA_Brochure_v8.pdf*
14. *Fox N.J., Postmodern reflections on 'risk', 'hazards' and life choices, in Risk and sociocultural theory: new directions and perspectives, ed. Lupton D., University Press Cambridge, UK, 1999, pp. 12-33*
15. *Iancu S.C., Mondoca N.R., Risk in Romanian businesses. Scientific Communications Session SECAAB 2006.*
16. *Iloiu, M., Risk and Risk Management, Annals of the University of Petroşani. Economics vol. V, Editor Universitas, Petroşani, ISSN 1582-5949, 2005*
17. *ISO Guide 73:2009, Risk management - Vocabulary*
18. *ISO/IEC 31010:2009 Risk management - Risk assessment techniques*
19. *ISO PAS 28000 Specification for security management systems for the supply chain- publicly available specification*
20. *Jorion, P., Risk Management, Annual Review of Financial Economics, Vol. 2, December 2010, DOI: 10.1146/annurev-financial-073009-104045, pp. 347-365*
21. *Lupton, D., Theorizing Risk, In Risk, Key Ideas, D. Lupton, ed., Rutledge, London, 1999a, pp. 18-36*

22. *Lupton, D., Risk, Rutledge, London, 1999b*
23. *Nicolescu O., Verboncu I., & Profiroiu M., Romanian Management Health State in 2010 Editura Pro Universitaria, Bucuresti, 2011*
24. *Public Finance Ministry, Order 946/2005 of regarding the approval of the Internal/managerial Code of control - including the internal control standards for public entities, Monitorul Oficial nr. 675, Anul 173 (XVII), republished in Monitorul Oficial nr. 469/5 iulie 2011*
25. *Standard ISO 31000:2009, Risk management – Principles and guidelines*
26. *Suciu G., Trifan A., Prevention of company risks, Annals of the „Constantin Brâncuşi" University of Târgu Jiu, Economy Series, Issue 5/2014, available at http://www.utgjiu.ro/revista/ec/pdf/2014-05/20_Suciu,%20Trifan.pdf, accessed in March 12 2015*
27. *Toma S.V., Chitită M., & Şarpe D., Risk and Uncertainty, Procedia Economics and Finance, 3, 2012, Elsevier Ltd., doi: 10.1016/S2212-5671(12)00260-2, pp. 975-980*
28. *http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref1586, accessed in March 25 2015*
29. *http://www.safetyrisk.net/wp-content/uploads/downloads/2010/12/SARM-Final.pdf, accessed in March 31 2015*