ACRN Journal of Finance and Risk Perspectives
Vol. 3, Issue 3, November 2014, p. 1 – 14
ISSN 2305-7394

CHALLENGES IN IMPLEMENTING ENTERPRISE RISK MANAGEMENT

Dornberger Kerstin[1], Oberlehner Simone[2], Zadrazil Nicole[3], Othmar M Lehner[4]
[1, 2, 3,4] Controlling, Accounting and Finance at University of Applied Science, Upper Austria

Abstract: *Since the financial crisis in 2008 organisations have been forced to rethink their risk management. Therefore entities have changed from silo-based Traditional Risk Management to the overarching framework Enterprise Risk Management. Yet Enterprise Risk Management is a young model and it has to contend with various challenges. At the moment there are just a few research papers but they claim that this approach is reasonable. The two frameworks COSO and GRC try to support Enterprise Risk Management. Research does not provide studies about their efficiency. The challenges of Enterprise Risk Management are the composition of the system, suitable metrics, the human factor and the complex environment.*

Keywords: *Traditional Risk Management; Silo; Enterprise Risk Management; ERM; COSO Cube; Governance, Risk and Compliance; GRC*

Introduction

The consideration of organisational risk has developed significantly during the past decade. Therefore different events have influenced this development, like corporate bankruptcies in 2002, which resulted in a passage of the Sarbanes-Oxley Act. This passage makes the board of directors and the executive management more responsible for corporate risk. Another example is the financial crisis in 2008, which made people aware of the importance of risk management. Entities started to change their silo-based traditional risk management to the enterprise risk management approach. Silo-based means thinking in containers, some departments of a company do not share information with other departments. The opposite of this silo approach is an integrated view that considers risk from the perspective of a whole organisation, which is called Enterprise Risk Management (ERM) (Connair, 2013).

The *Chartered Institute of Management Accountants (CIMA)* published a report which warned against the silo mentality. The report shows three important weaknesses of the silo-mentality. The first shows that risk was being monitored in individual divisions but the overall risk could develop unchecked. The second weakness of this approach is the possible development of an aggressive risk culture. The last weakness is the dependence on mathematical risk models, which can be dangerous, because the model probably accepts risks at certain levels, yet entities should not accept it in their everyday operations (CIMA, 2010).
There are two frameworks to support the Enterprise Risk Management approach – the COSO Cube ERM and the Governance, Risk and Compliance (GRC) model. The Committee of Sponsoring Organisations established the COSO Cube to support ERM (COSO, 2004). The GRC model is another framework and it is a paradigm to help an entity to grow in the best possible way (Moeller, 2011).

In the following the implementation of ERM, the two mentioned frameworks and the possible challenges will be discussed.

Enterprise Risk Management

Enterprise Risk Management is defined as an overarching framework and it is a structured analytical process that concentrates on identifying and eliminating the financial impact and volatility of a portfolio of risks. The importance is that every risk can be seen as an opportunity to gain competitive advantage (American Society for Healthcare Risk Management, 2006).

Another study investigated the efficiency of ERM-systems during the financial crisis. Different organisations were divided into three stages: strong, weak and no ERM-system. The outcome of this research is that organisations with a strong ERM-system could outperform organisations with a weak or no ERM-system. Organisations with no ERM-System could outperform as well organisations with a weak system. Therefore it is recommended to have a strong ERM-system and to implement it properly (Seik/Yu/Li, 2011).

Implementation of ERM

To be able to implement ERM, an organisation has to educate their staff (American Society for Healthcare Risk Management, 2006). To have an effective Enterprise Risk Management, an enterprise risk management function should be established and headed by a chief risk officer, short CRO. The CRO has to coordinate risk management efforts and report to the Board of Directors (Lindberg/Seifert 2011).

In a second step an entity needs to know its goals and objectives before the management can identify events that might interfere with the entity's objectives (American Society for Healthcare Risk Management, 2006).

To be effective, the CRO and the ERM-function need to be aware of the various levels of risk that have an impact on all levels of an enterprise. An effective ERM-function should be covered by professional staff with an understanding of the risks influencing the enterprise and knowledge of techniques to limit risk. In addition to an effective risk function, a series of policies and standards for risk management should be established and communicated (Duckert, 2010).

According to *Kennedy* there are five steps to do ERM right:

1. "*Establish governance and expect it to change.*
2. *Start the conversation inside and outside.*
3. *Use risk management tools and methods*
4. *Keep line of sight from actions to root causes to risk.*
5. *Share findings across domains.*" (Kennedy, 2008)

According to COSO ERM Frameworks study, ERM is already an accepted approach to deal with business wide risks; however the stage of most ERM systems is still very immature. Only a few organisations already implemented a systematic, robust and repeatable process of ERM. A large number of organizations is still not satisfied with their process of risk assessment and need further guidance in implementing ERM (Beasley/Branson/Hancock, 2010a).

Support: COSO Cube and GRC

As aforementioned, the implementation of ERM is a challenging and resources- and time-consuming task. There are no step-by-step instruction manuals, and studies about practical issues are very rare. However, certain organisations are trying to support entities in implementing ERM by providing frameworks and guidance. Two well-known frameworks are COSO Cube ERM and GRC. Referring to literature research this chapter tries to define their structure and effectiveness. Furthermore, a critical appraisal is trying to find out any shortfalls or necessary improvements.

COSO Cube ERM (2004)

The Committee of Sponsoring Organisations was organised in 1985 by 5 main sponsors. Its main task is to provide frameworks and guidance to implement ERM and internal controls in order to reduce the extent of fraud (COSO, 2004). This article will focus on the ERM framework.

Entities shall be supported to implement an Enterprise Risk Management by the COSO Cube ERM. Its focus is set on different functions that establish an effective risk management. Firstly, the foundation of this framework is the alignment of entities' risk appetite and strategy. The management evaluates strategic alternatives, settles related objectives and develops mechanisms to manage related risks taking into account the risk appetite. Based on the risk appetite an entity is also able to enhance risk response decisions: risk avoidance, reduction, sharing or acceptance. Due to a more and more complex environment, an efficient ERM enables reducing operational surprises and losses. Most risks are related today, ERM again support to deal with multiple and related risks within an entity. ERM not only handles risks, it also identifies opportunities and tries to realize them (COSO, 2004).

Setup and definitions

This framework is a 3 dimension matrix, as you can see in the graphic below.

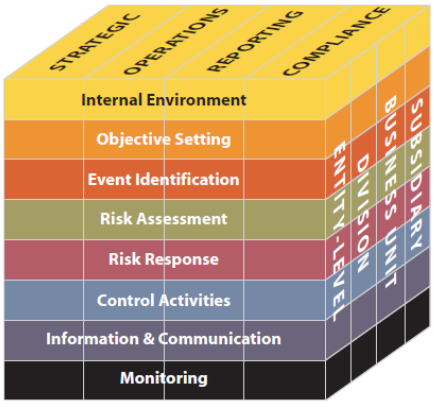

Figure 1: COSO Cube ERM 2004, source: COSO ERM Framework, 2004

On top, an entity has to select a strategy and establishing aligned objectives cascading through the entity. These objectives are set in four different categories. Strategic objectives are high-level goals, aligned with and supporting its mission. Operational objectives enable an effective and efficient use of entities' resources. Reporting objectives ensure the reliability of the reporting system and compliance objectives need to meet all law and regulation requirements (COSO, 2004).

On the front side the 8 main interrelated components of Enterprise Risk Management are described. The internal environment determines the philosophy and how risk is viewed within and organisation. Furthermore, it sets ethical values, integrity and, the risk appetite of an enterprise. As risk appetite is the foundation of the following components, its determination needs to be carried out very carefully. Risk appetite is the amount of risk an entity is willing to take entirely. It is a reflection of the entities' risk management and influences the culture within an organisation (COSO, 2004).

There is no "standard" risk appetite that applies to all organisations. As organisations set different objectives, their risk appetite is diversified as well. Furthermore, an organisation must understand the impact of determining higher and lower risk tolerance levels for certain objectives. An organisation needs to communicate those levels to ensure an effective ERM. Finding the right approach to do this is a challenging task. Three different approaches have proved to be successful. Firstly, an organisation could create an overall risk appetite statement. It should be broad enough, yet descriptive enough for organisational units to manage their risks within. The second approach is to communicate risk appetite for each material class of organisational objectives. Another approach is the communication of risk appetite for different categories of risk. Finally, risk appetite needs to be reviewed continuously as the environment is changing to the same extent. You can see the whole process below

Figure 2: Risk Appetite. Source: Rittenberg/Franks, 2012

(Rittenberg/Martens, 2012).
According to COSO Cube ERM the next step is to set certain objectives. Otherwise it would be impossible to identify any risks or opportunities. These objectives must be in alignment with the strategy and mission of the organisation. The management is responsible for the objective setting (COSO, 2004).

Afterwards, it is necessary to monitor the internal and external environment for any events that may be a threat in achieving objectives or opportunities. Opportunities need to support the mission and strategy of an organisation. Then, any risks get analysed, considering likelihood and impact to determine how they should be managed. Risks get assessed on an inherent and a residual basis. Otherwise, an organisation would not be able to find the right risk response. Management has to decide whether to avoid, accept or share a certain risk. To do so, it develops a set of actions to align risks with the entity's risk tolerances and risk appetite. Control activities are necessary to find out if risk responses are effectively carried out (COSO, 2004).

All tasks above could not be achieved, if the relevant information was not identified and communicated efficiently, so responsible managers could react immediately. Finally, the entirety of ERM needs to be monitored continuously to improve it when necessary (COSO, 2004).

The relationship of the different objectives and components is essential. An entity strives to achieve its strategic, operational, reporting and compliance objectives by establishing all eight components of ERM in an efficient and effective way (COSO, 2004).

Critical appraisal

Up to today, there has not been any real evidence that the COSO ERM frameworks actually improve or enhance firm value. Over the course of the last years only a few studies have considered the effectiveness of the COSO ERM Framework. In *The Adoption and Design of Enterprise Risk Management*, Leen PAAPE and Roland F. SPEKLÉ considered the effect of the ERM design on risk management effectiveness for the first time. They carried out an empirical study in the Netherlands. 825 organisations in the Netherlands were the sample size. This sample size included large organisations, SMEs and the public sector as well. All of them implemented ERM by different designs at different stages. In general, the main point of criticism for this framework is that there is a very broad guidance. It contains not more than some key principles but organisations have to work them out by themselves (Paape/Speklé, 2012).

COSO determined 3 important factors that increase effectiveness. Those are the frequency of risk assessment, the chosen techniques to measure risk and the time frame of reporting (COSO, 2004). Yet, the study stated that there are far more factors necessary to implement an effective ERM system. It is clear that those are important factors, but most organisations need more support in certain parts of the framework. A big issue in practice is the determination of the risk appetite. Shall a risk appetite be determined in a qualitative or a quantitative way? How shall risk appetite be in alignment with objectives of an organisation? COSO issued a special paper dealing with risk appetite but again, there was a very broad guidance, and determination of risk appetite is still a challenge. According to risk assessment, most organisations are not sure about how often they should go over the risks. Organisations call for a minimum level for the frequency of risk assessment at least. The localisation of ERM is another important challenge in implementing an ERM system. According to COSO risk management is the task of every single person within an organisation. That is a huge contradiction in this framework as ERM would not be carried out efficiently if everyone was responsible. Frequently asked questions are who is responsible for ERM in general and on different management levels. The last critical issue was that according to COSO a highly sophisticated IT and information system is necessary in the first place to carry out ERM. However, there is not any support to develop such a system (Paape/Speklé, 2012).

All in all, most organisations need more detailed guidance to implement COSO. According to Paape/Speklé ,about 43 % use the COSO ERM framework, but they did not outperform organisations with another design of ERM. Just using the COSO framework does not contribute to the effectiveness of ERM (Paape/Speklé, 2012).

GRC

Another model to implement ERM is GRC. It consists of three main principles. Those principles are Governance, Risk and Compliance. The collapse of the energy trading firm Enron, due to its accounting scandal, and the housing market collapse led to an improvement for compliance requirements. A few years after introducing Sarbanes-Oxley Act, GRC was

first mentioned by PwC in 2004. Nowadays, the Open Compliance and Ethics Group (OCEG) is responsible for support and guidance to implement GRC. Referring to literature research, this chapter tries to define their structure and effectiveness. Furthermore, a critical appraisal is trying to find out any shortfalls or necessary improvements (Moeller, 2011).

Setup and definitions

G – Governance

Corporate or enterprise governance refers to the rules, processes or laws by which an organisation operates and controls. That term can be defined by certain officers, stockholders and basic objectives of an organisation, internal factors, but by consumer groups, clients and government regulations, and external factors as well. The goal of the governance principle is to provide a strategic direction and to ensure an achievement of an organisation's objectives. It is a process of establishing rules and procedures within all levels of an organisation and communicating them to relevant stakeholders. Furthermore, the organisation gets monitored according to those rules, and all rewards are determined by the performance of an organisation against those rules. Due to recent scandals concerning the misuse of enterprises, power governance has become more and more important. To establish a reliable and effective Governance system is a challenge all organisations need to face (Moeller, 2011).

R – Risk

The risk principle is very similar to the COSO ERM framework, as you can see in the graphic below.

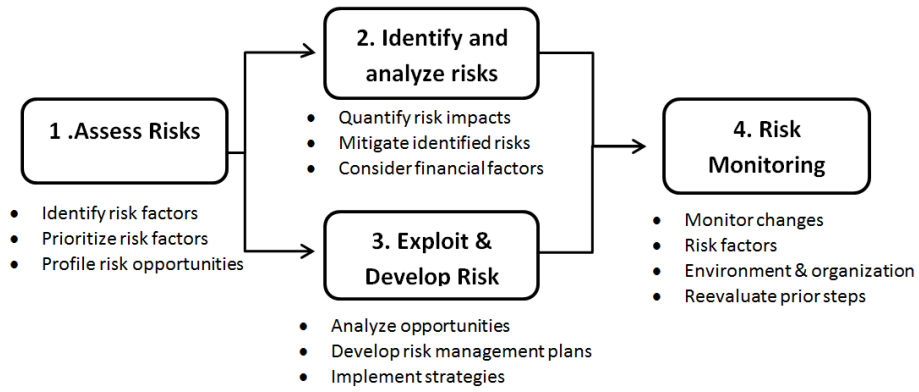

Figure 3: Setup Risk Assessment. Source: own graphic referring to Moeller, 2011

In risk assessment and planning it is necessary to face all levels of risk, whether on a global basis or certain operational risks. It is not possible to identify all risks threatening an organisation but there should be an ongoing analysis. By risk identification and analysis all identified risks get valued by their likelihood and impact on an organisation. Afterwards it is possible to develop sufficient risk response strategies. All identified risks finally need to be monitored continuously to react as soon as possible if there were changes in likelihood. The critical issue is to keep ahead and to adjust risk responses (Moeller, 2011).

In general, risk management should create value and enhance stakeholder's value. Furthermore, it should be an integral part of organisational processes, so it should be part of the decision-making process. RM also needs to be tailored in a structured manner to address

the uncertainties an enterprise faces based on the best available information. Finally, RM needs to be dynamic, iterative and responsive to changes in the environment (Moeller, 2011).

C – Compliance

This principle is the process of meeting the requirements of certain laws and regulations as well as of internal corporate policies. It is a very complex task as there are many uncertainties and challenges. First of all, new regulations are introduced frequently; subsequently they need to be adapted continuously. Next, many regulations are vaguely written, so an interpretation is required. Furthermore, many regulations do not support thrift. For example: There is the regulation "All transactions must be supported by a receipt". It would not be efficient to draw up a receipt for amounts less than e.g 10€ within a multinational organisation. Also, multiple regulations often overlap as different geographical locations are involved. Finally, already existing regulations change continuously, subsequently a strict compliance is hard to establish. Therefore, compliance is an ongoing process and not a one-time project (Moeller, 2011).

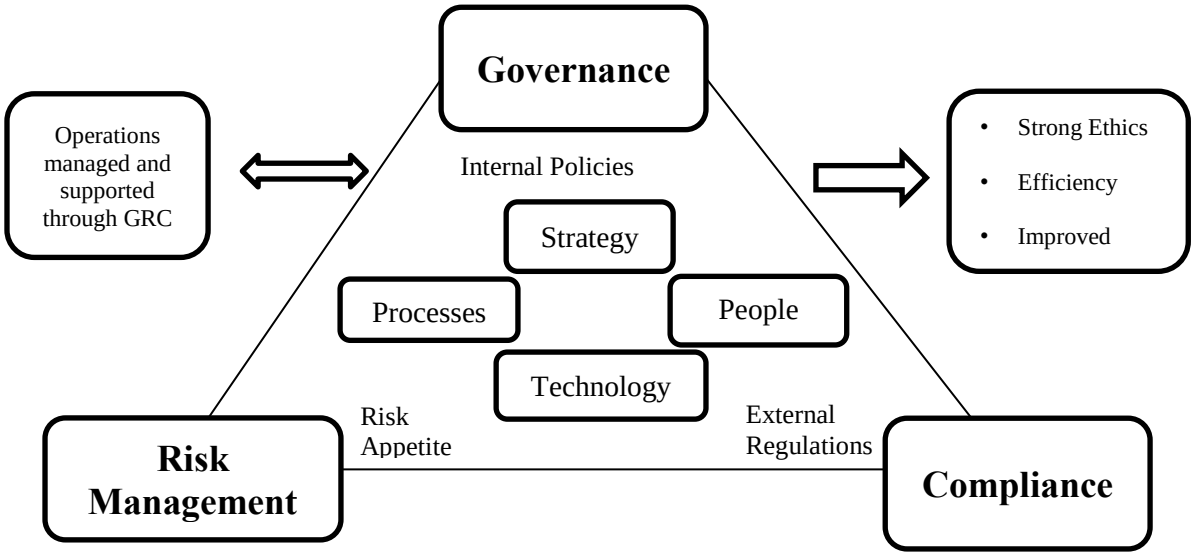

Figure 4: Governance, Risk and Complience. Source: Moeller, 2012

Critical appraisal

The most common failure of organisations is to deal with those principles separately. They think this is the only thing to do to take care of an organisation, but it is so much more. It is a paradigm to help an organisation grow in the best possible way, and these principles need to be integrated in one another. Each principle consists of four basic GRC components: Strategy, Processes, People and Technology. Those components are necessary for this framework to work. The different principles get either supported by internal policies, risk appetite, or by external regulations. All operations need to be managed and supported by the GRC principles in order to state strong ethical values, to ensure efficiency and to improve the effectiveness of an organisation (Duckert, 2010).

Many experts say that a holistic, strategic, and integrated approach to GRC shall enhance value and strengthens the competitiveness of an organisation. So far, studies to prove this statement are very rare. In *Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey among Large Enterprises,* researchers tried to find out the significance of the GRC model in large enterprises in 2010. That framework implies

integration across and within its four components: strategy, processes, people and technology. Only a third of organisations accomplished to integrate the strategy in their GRC framework. In general, only 37 % of all organisations researched understand the value and service of the GRC model and implemented it. A fifth does not even consider GRC. The rest is quite uncertain about its importance, so there is high number of organisations without a GRC framework. Furthermore, many organisations are not capable to implement an integrated framework and still handle the three silos separately. Only a few of them implemented a central GRC department as there are lots of organisational hurdles to overcome (eg. IT support). Even in organisations with a GRC system, there is high potential to optimise that system. Many organisations may ask, if this is worth the effort, as there is still no scientific proof for the benefits of an integrated GRC model. No business cases have been created yet, and theoretical models are more than vague about promised benefits. Furthermore, the description of those benefits is very broad. It is hard to measure an ethically correct behaviour, an improved efficiency and effectiveness of all components. Only 5 % of all organisations achieved benefits of a GRC system as they aligned daily operations with their strategy and established a more transparent risk management. However, organisations with a strong GRC system increased their competitiveness as they are attributed a more positive image by their customers. That resulted in better customer relationships and higher sales (Raczs et al., 2010).

In 2012, again, large companies were questioned for their progress in implementing GRC systems. All in all, the number of highly integrated GRC systems within all principles is still very low. However, the number of organisations implementing and optimising GRC is growing. Additionally, more organisations are able to achieve benefits. The most challenging hurdle is still the integration of all principles and to overcome lacks (OCEG, 2012).

In general, implementing GRC is a highly sophisticated task. Most organisations cannot see any benefit, but a high amount of costs. Those costs are only caused if GRC is not implemented correctly. To grow value out of GRC, organisations need to meet certain requirements:

- more analytics
- more integration with more automated monitoring of risks and controls
- more content
- more services

To build an effective and efficient GRC model out of this, five architectural principles shall be followed:

- simplicity
- effectiveness
- alignment
- accountability
- consistency (Caldwell, 2012)

However, there is still no step-by-step guidance to implement GRC, and it will still take many years for organisations to implement or optimise their system (Caldwell, 2012).

Challenges

There are five main aspects that cause mistakes when implementing an Enterprise Risk Management tool. Firstly, the system itself can be inappropriate. The second factor deals with "human errors", the third factor is the complexity of the environment. The next factor deals with the challenges in identifying risks which is linked to the last part the metrics.

Challenges in General

This paper will discuss potential errors of tools; a challenge could be to find the *perfect framework*. The frameworks COSO and GRC have been mentioned above, but there are more different types of frameworks, for example AIRMIC, Combined Code on Corporate Governance, FERMA and others. The decision for an appropriate framework includes the selection of an appropriate risk framework and the implementation into the organisation. Some of the frameworks have advantages, such as workbook materials and display slides that may help the implementation process. Internal auditors can help a management evaluate which are best suited to the organisation's needs. Related to that, *the technologic part* is important as well. Many risk management packages use a methodology that is not specifically based on the framework. If that happens, the deficiencies can lead to difficulties. Technology should be built around the methodology and used in several ways. Another impact could be that the *Human Resource is not integrated* in the ERM System. From the Human Resource's view, specific goal-setting tied to the success of ERM must be part of an individual's performance management plan. If this is not done, the implementation exercise could fail. The business strategy should be defined at the outset of the exercise along with the organisation's mission and vision. The ERM process will flow forward from this strategy, and events will be identified that may impact the achievement of the organisation's strategies and objectives (Schanfield/Helming, 2008).

Human Errors

To ensure that the framework suits an organisation, the human factor needs to be minimised. There are different types of human errors. Therefore, the next section will focus on the different types and their impacts. One problem for both tools (GRC and COSO-Cube) could be that not everyone is "*on the same page*". That is why the project team should develop a risk glossary at the beginning of the ERM implementation process, so the company can save money and time. The risk management team has to *agree on definitions* for risks, risk assessment, risk management, ERM, significance, likelihood, inherent risk and residual risk. Afterwards it is very important to define what risk really means for the entire organisation, because there are several different interpretations. After this process, when the team is at the same level, they can go on. *Effective monitoring* needs to ensure that the agreed-upon risk response is actually implemented and working. It is important to clarify monitoring responsibilities among internal auditing, individual business managers, and the board. Software based on key performance metrics may be used to design an effective continuous monitoring process. *A risk-aware culture* is necessary to ensure that the risk process becomes institutionalised within the organisation. More advanced risk identification techniques, such as control self-assessment, may be adopted eventually. Decisions and actions within the organisation must be viewed within the context of a team approach. Moreover, each team member authority and responsibility for risk must be spelled out. The last step is to

communicate the most important impacts to the rest of the organisation. So the entire organisation understands the benefits they gain from implementing an ERM model (Schanfield/Helming, 2008).

Complex Environment

Different studies state that the main reason for a complex environment is that the world faces VUCA (volatility, uncertainty, complexity and ambiguity).Volatility is the nature and dynamics of change, and the nature and speed of change forces and change catalysts. Uncertainty points out the lack of predictability of issues and events. Complexity is the confounding of issues and the chaos that surrounds organisations. Ambiguity is the haziness of reality and the mixed meaning of conditions, cause-and-effect confusion (Horney/Pasmore/O'Shea, 2010). Especially according to evaluating and measuring risks it is necessary to know what could happen in the environment. Tsunamis, earthquakes, hurricanes, tornadoes and terrorism affect organisations worldwide. In those past years there were several examples of that, and each inevitably affected the distribution of global supply chains. (Schlegel/Trent, 2012). For example the earthquake in Japan 2011 caused a Tsunami, which resulted in several explosions and finally a nuclear meltdown at the Fukushima nuclear power plant. Afterwards the Chancellor of Germany, Angela Merkel, decided on a nuclear phase out for Germany. This impact for the atomic power industry was hardly predictable (Guwak, 2012).

Challenges Related to the Process

The process from identifying risks to monitoring risks means a lot of challenges. The next section focuses on challenges that could occur in that process. Afterwards the chapter "Metrics" will explain how metrics can support this process.

Figure 5: Risk Process. Source: Schanfield/Helming, 2008

Mostly the problems occur when *identifying risks* because that has to be done by a Risk-Management-Team. The team has to systematically collect information on all risks and types of risks. It is important to uncover all risks, because undetected risks can influence the organisation (Posch/Nguyen, 2012). Consequently, the team has to understand the techniques for identifying risks. The process should include reviews of prior internal audit reports, risk questionnaires, brainstorming, business studies, scenario analysis and more. It is helpful to interact with internal and external stakeholders. For example the term "risk questionnaires" can include questions in several areas, such as operation, information/IT, finances, regulations, economics, competition, strategy, litigation and catastrophe. Concerning regulations, questions such as: "What regulations apply to the organisation?", "Has it ever been audited by an external agency?", "Are copies of such audit reports available?" and others might be asked. For *assessing risk* it is important to take the significance and the likelihood of risk events into account. There are qualitative, semi-quantitative, and quantitative techniques available to assess the risk in the best way. The challenge here is to determine an appropriate technique or combination of techniques so that the various risks can be taken care of effectively. Afterwards it is difficult to *quantify the risk*, the auditors must keep in mind that just because something cannot be quantified in monetary terms, it does not mean that the risk will never occur and does not exist. For example the governance risk cannot be quantified easily, although governance activities can highly influence an organisation. After risks are

implemented in the risk assessment, the risk has to be *evaluated*. To evaluate the risks they have to be prioritised and afterwards compared with the established risk tolerance. The next challenge for the management is to *treat the risks*. As already mentioned in the step before, it is necessary to produce a comprehensive list of all risks and tolerances. Afterwards the organisation has to take action on the risks that exceed the tolerance line. The board may have to re-examine tolerances if many of the risks identified exceed them. The risk treatment options are: Accept risk, avoid risk, outsource, share, transfer or remedy risk. These steps have to be individualized by the organisation itself (Schanfield/Helming, 2008).

Metrics

In the following, two different types of metrics are described. The first, the identification of key risk indicators, belongs to the first step - identifying risks - in the risk process. The second type is the scoring model, and it belongs to the step "evaluating risks".

Identification of key risk indicators

To increase the effectiveness of an Enterprise Risk Management process and to improve the accomplishment of an organisation's strategy, the management needs to develop effective key risk indicators (KRIs). Therefore the awareness of risk can be heightened. The first step of developing an effective set of KRIs is to identify metrics that can provide useful information about potential risks. A link between the top risks and the core strategies can help to illustrate relevant information that could be a leading indicator of an emerging risk. The illustration shows that the management aims to achieve greater profitability by increasing revenues and reducing costs. The management identified four strategic initiatives to reach those objectives. Out of these initiatives some potential affective risks have been identified. The management team has to start to identify the most critical metrics. These metrics can be the leading key risk indicators to oversee the accomplishment of strategic initiatives. The KRIs have been identified for each critical risk. This mapping of strategic initiatives, potential risks and key risk indicators can help the management to have an overview and not to be misled by irrelevant information (Beasley/Branson/Hancock, 2010b).

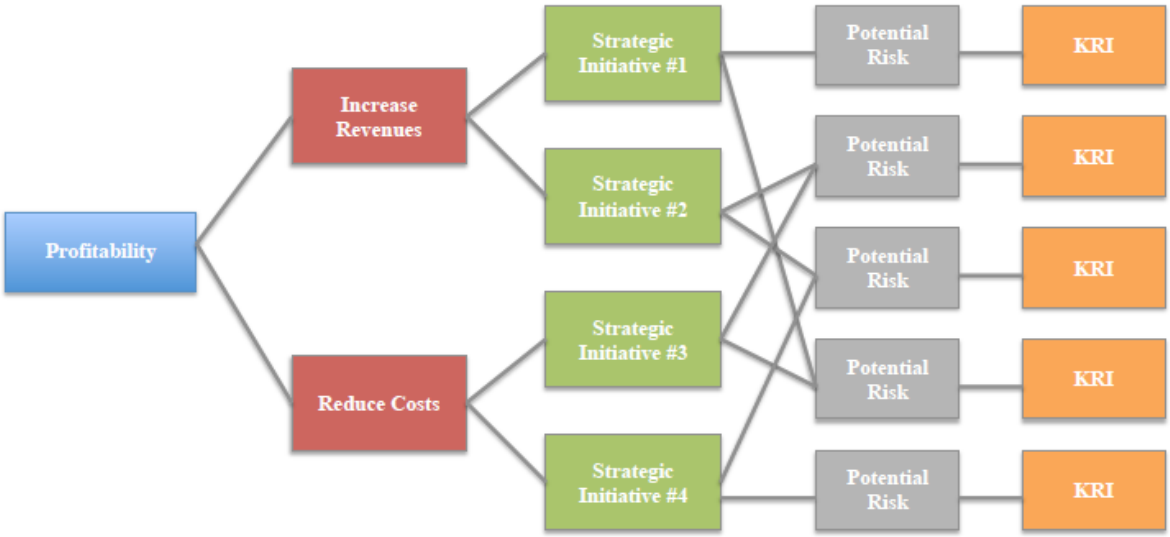

Figure 6: Key Risk Indicators. Source: Beasley/Branson/Hancock, 2010b

Effective KRIs can provide useful information and value to an entity in different ways. Potential value can be derived from each of the following contributions:

- Risk Appetite
  KRIs can be a useful tool for better articulating the risk appetite that represents the organisational mindset in the best way

- Risk and Opportunity Identification:
  KRIs can be designed to warn the management team or to even show opportunities

- Risk Treatment
  KRIs can set off actions to mitigate developing risks. They can also serve as controls by fixing limits for certain actions.

- Risk Reporting
  Summary reports can be quickly communicated to the board of directors by KRIs.

- Compliance Efforts
  KRIs can be useful for demonstrating compliance in areas like reserve levels (Beasley/Branson/Hancock, 2010b).

Scoring model

Risk can sometimes be difficult to calculate. It then becomes a qualitative indicator and it is rated e.g. as low, middle and high. The qualitative results are then assigned numbers again, which is called a quantification of qualitative factors (scoring). This quantification is called a scoring model. One example of that is to quantify the level “excellent“ with ten points and grade down to level “insufficient“ with zero points. Furthermore, some criteria can be weighed different to distinguish the importances of risk. (Hertenberger, 2007)

Scoring models are versatile and easy to implement. These models allow a multi-dimensional evaluation and comparison of different alternatives. According to *Diederichs,* a criticism of the model is that it can hardly be objective. Defining criteria, weighing, and final scoring include some subjective evaluations. Yet in research it is seen as a suitable model to evaluate risks (Diederichs, 2013).

Conclusion

Risk management has always been an important part in organisations, but since the Sarbanes-Oxley-Act of 2002 it has become obligatory. After the financial crisis in 2008, organisations moved away from the silo-based Traditional Risk Management to the Enterprise Risk Management. In comparison to the TRM, ERM is seen as an overarching framework dealing with all kinds of risks. Research papers state that a change was necessary because the silo-based approach only deals with financial aspects. ERM is a more complex approach but supposed to enhance more value for the stakeholders. The initial step to implement ERM is to announce a centralised risk department led by the chief risk officer. The last step of the process is a report to the board of directors by the CRO.

In general, the establishment of ERM processes is highly sophisticated. Different organisations try to support entities with their frameworks, like COSO Cube ERM and GRC. Both frameworks are a very broad guidance and entities still struggle in implementing ERM. Furthermore, certain research papers state that there is no scientific proof of their effectiveness yet.

One challenge of the implementation is to find the proper framework for an entity supported by a suitable IT-system. Even if some risks are hard to quantify, an organisation should not exclude them. According to research it is necessary to face human errors and to

minimise this factor along the whole process. The entity shall be aware of the complex environment and its impact on the organisation.

Especially the risk process contains important challenges in risk identification, risk assessment, risk evaluation, risk treatment and risk monitoring. To start the process and to identify risks an entity should determine the appropriate key risk indicators.

Furthermore, the development of a scoring model is a way to evaluate risks even though this model can include subjective estimations.

To sum it up, ERM is still a new approach and needs further research. Organisations should not expect an overall step by step guidance or any best practices. Every entity has to face different risks so every ERM system need to be different as well. Subsequently, a general ERM system suitable for any kind of organisation seems to be impossible.

Instead of waiting for best practices or further guidances organisations shall put more effort in developing their individual ERM system. That system could be designed by COSO Cube or GRC, but an organisation shall not get tied up over the question what if those frameworks do not work out 100 percent for a certain organisation. If this might be the case, organisations shall not hesitate and adapt their system and establish their own best practice.

References

Beasley, Mark/Branson, Bruce/Hancock, Bonnie (2010a): Current State of Enterprise Risk Oversight and Market Perceptions of COSO's ERM Framework In: COSO Thought Leadership in ERM – COSO's 2010 Report on ERM.

Beasley, Mark S./Branson, Bruce C./Hancock, Bonnie V. (2010b): Developing Key Risk Indicators to Strengthen Enterprise Risk Management. How Key Risk Indicators can Sharpen Focus on Emerging Risks. In: COSO Thought Leadership in ERM.

Caldwell, French (2012): 5 principles for effective GRC. [WWW] https://exchanges.nyx.com/allison-orourke/5-principles-effective-grc-programs (10.4.2014)

CIMA (2010): Risk Management report warns against silo mentality. In: Insight. Incorporating Synergy. The e-magazine for management accountants. [WWW] http://www.cimaglobal.com/Thought-leadership/Newsletters/Insight-e-magazine/Insight-2010/Insight-September-2010/Risk-management---what-went-wrong-at-RBS/ (10.4.2014)

Connair, Stephen (2013): Enterprise Risk Management. From Silos to Strategic Objectives. In: Armed Forces Comptroller. Page 24-26.

COSO (2004): Enterprise Risk Management – Integrated Framework – Executive Summary

Diederichs, Marc (2013): Risikomanagement und Risikocontrolling.

Duckert, Gregory H. (2010): Practical Enterprise Risk Management: A Business Process Approach

Guwak, Barbara (2012): CFO aktuell Heft-Nr 4/2012: Die Welt ist VUKA

Hertenberger, Simon (2007): Risikomanagement. Vortrag in der Seminarreihe „Statistische Mechanik der Finanzmärkte" im WS 07/08

Horney, Nick/Pasmore, Bill/O`Shea, Tom (2010): People & Strategy: Leadership Agility: A Business Imperative for a VUCA World

Kennedy, Peter (2008): Enterprise risk management: effective ERM practices. Strategy & Leadership, Vol. 36 Iss: 3

Lindberg, Deborah L./Seifert, Deborah L. (2011): Enterprise Risk Management (ERM) Can Assist Insurers in Complying with the Dodd-Frank Act.

Moeller, Robert R. (2011): COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes

NYSE EURONEXT Exchanges (2012): 5 Principles for Effective GRC Programs. [WWW] https://exchanges.nyx.com/allison-orourke/5-principles-effective-grc-programs (10.4.2014)

OCEG (2012): GRC Maturity Survey & Research [WWW] http://www.oceg.org/downloads/grc-maturity-survey-research-2012.pdf (12.4.2014)

Paape/Speklé (2012): The Adoption and Design of Enterprise Risk Management – Practices: An Empirical Study. In: European Accounting Review Vol. 21, No. 3, 533–564, September 2012

Posch, Peter N./ Nguyen, Tristan (2012): Risikoidentifikation und Riskioinstrumente im Rohstoffmanagement

Racz, Nicolas/Panitz, Johannes C./Amberg, Michael/Weippl, Edgar/Seufert, Andreas (2010): Governance, Risk & Compliance (GRC) Status Quo and Software Use. Results from a Survey among Large Enterprises.

Rittenberg, Larry/Martens, Frank (2012): Understanding and Communicating Risk Appetite. In: COSO Thought Leadership in ERM

Schanfield, Arnold/ Helming, Dan (2008): 12 Top ERM Implementation Challenges: Internal Auditor

Schlegel, Gregory/ Trent, Robert (2012): Risk Management: Welcome to the new normal

Seik, Heng Yik/Yu, Jifeng/Li, Jared (2011): Enterprise Risk Management in Financial Crisis.