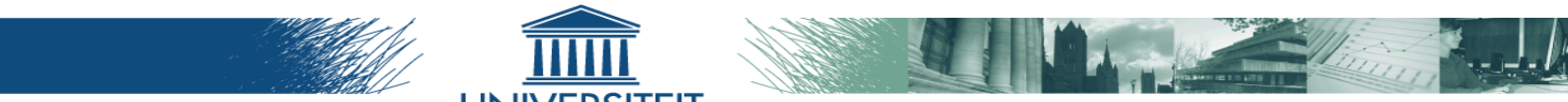


UNIVERSITEIT GENT

FACULTEIT ECONOMIE EN BEDRIJFSKUNDE

ACADEMIEJAAR 2011 – 2012

Risk management in non-financial companies in Belgium:

A state of affairs

Masterproef voorgedragen tot het bekomen van de graad van

Master of Science in de Toegepaste Economische Wetenschappen

Laurien Van den Meerssche

Julie Van Heghe

onder leiding van

Prof. Dr. Regine Slagmulder

PERMISSION

We declare that the contents of this thesis may be consulted and/or reproduced, provided that the source is acknowledged.

Ondergetekenden verklaren dat de inhoud van deze masterproef mag geraadpleegd en/of gereproduceerd worden, mits bronvermelding.

Laurien Van den Meerssche

Julie Van Heghe

Acknowledgements

We want to take special time and make space to thank all the people and organizations that helped us to make our thesis a piece of work we are proud of.

First of all, we want to thank our promoter, Prof. Dr. Regine Slagmulder, for giving us the opportunity to work with her. We are very grateful to her for her input that moved our thesis in the right direction. Thanks to the guidance of Prof. Slagmulder, our thesis has become a nice accomplishment in our Master year.

Belrim, the organization that really helped us to get the respondents on our on-line enquiry, deserves also a special thank you from us. Thank you Dr. Marie-Gemma Dequae for your cooperation, from the beginning until the end of our thesis.

We interviewed people in two companies who we also want to thank, with a special thank you towards the first ones for the thoroughly given information and explanation.

Another acknowledgement goes out to all the companies that made time to complete our questionnaire.

Last, but certainly not least, we also want to show our appreciation for our parents for their support and all the opportunities they have created for us. We could not have done this without them.

Thank you.

Laurien and Julie

Dutch Summary

Risicobeheer is een actueel onderwerp in de snel wijzigende hedendaagse economische omgeving. Iedere onderneming zou risicobeheer moeten implementeren in zijn bedrijfsactiviteiten omwille van de vele voordelen en opportuniteiten die het kan creëren. Het kan bijvoorbeeld de waarschijnlijkheid op potentieel succes verhogen, de kans op faling van de onderneming reduceren en de onzekerheid om de ondernemingsobjectieven te verwezenlijken, verminderen. Risicobeheer is een concept dat recent veel aandacht verkrijgt, maar ondanks deze verhoogde belangstelling toch nog steeds niet voldoende geïmplementeerd wordt (Fall guys - Risk Management in the Frontline, 2010). In ons onderzoek proberen we op basis van 2 case studies en een online vragenlijst te achterhalen hoe ondernemingen aan risicobeheer doen en peilen we naar de kennis van de daarmee samenhangende concepten.

In de literatuurstudie worden de onderwerpen aangehaald die we later bevragen in het empirische gedeelte, om een stand van zaken te verkrijgen betreffende risicobeheer. Eerst en vooral wordt een omschrijving gegeven van de begrippen risico, risicobeheer en Enterprise Risk Management. Verder volgt er een weergave en beschrijving van een standaard risicobeheerproces, waarbij de verschillende stappen ervan worden aangehaald. De voornaamste technieken die in de literatuur voorkomen om risico's te identificeren evenals de procedures om deze risico's te managen, worden bondig beschreven. Tenslotte worden ook de verantwoordelijken voor risicomanagement, de taken en het wetgevend kader waarin risicomanagement toegepast wordt, belicht.

In het empirisch onderzoek gedeelte hebben we deze theoretische bevindingen vergeleken met de praktische implementatie. Hieruit blijkt dat het begrip 'risicobeheer' algemeen gekend is in de meeste ondernemingen. De risicoclassificatie in de vier categorieën, namelijk financiële, operationele, strategische risico's en risico's met betrekking tot naleving van de wetgeving, die regelmatig aan bod kwam in de literatuur, lijkt ook te worden toegepast in het merendeel van de ondernemingen. Uit de interviews met de twee ondernemingen blijkt dat deze categorieën kunnen worden aangevuld met bedrijfsspecifieke indelingen.

De Belgische ondernemingen beschikken bijna allemaal over een ERM programma dat de basis stappen i.v.m. risico-evaluatie en risicobehandeling bevat. Uit ons onderzoek blijkt dat risico identificatie, risico analyse en risicobeschrijving de meest frequent uitgevoerde stappen zijn. We stelden vast dat deze dicht worden opgevolgd door de risicobehandeling, monitoring en rapportering.

De logische stap na de risico identificatie is het op een gepaste wijze behandelen van de risico's. Een techniek die herhaaldelijk in de literatuur wordt omschreven, is de 'heat map'. Deze techniek stelt een matrix voor waarbij een risico wordt weergegeven op basis van zijn impact en de waarschijnlijkheid dat het zich voordoet. Dit kan zowel afzonderlijk voor elk risico worden uitgevoerd als in combinatie met andere risico's die ook kunnen voorkomen bij een bepaald project. Ondanks de aandacht die wordt geschonken aan deze techniek in de bedrijfsliteratuur, heeft 40 procent van onze ondervraagde bedrijven nog nooit van het begrip gehoord. Wel zagen we een voorbeeld van de implementatie ervan in de twee geïnterviewde bedrijven.

De meerderheid van de ondernemingen duidt de lijnmanager als verantwoordelijke aan voor het risicobeheer in hun onderneming. De lijnmanager wordt echter nauw opgevolgd door de Chief Risk Officer (CRO). Een opmerkelijke bevinding inzake deze verantwoordelijkheden is het feit dat in ondernemingen waar een CRO aanwezig is, deze daarom niet automatisch als verantwoordelijke wordt benoemd. Dit in contrast met de literatuur die aangeeft dat de aanwezigheid van een CRO leidt tot een verantwoordelijkheidsfunctie van de CRO ten aanzien van risicobeheer (Committee of Sponsoring Organizations of the Treadway Commission, 2004).

Uit de literatuur vloeit voort dat de wetgevende omgeving omtrent risicobeheer, gedomineerd wordt door het Committee of Sponsoring Organizations (COSO) en de International Organization for Standardization (ISO). Het COSO raamwerk wordt geïmplementeerd in de beide geïnterviewde ondernemingen, alhoewel de tweede onderneming geen grote aanhanger is van dit eerder theoretische model. Uit onze enquête blijkt dat 33 procent van de ondervraagde bedrijven het COSO raamwerk hanteert. Daarnaast merken we ook op dat een groot aantal ondernemingen een bedrijfsspecifieke standaard heeft geïmplementeerd. De ISO 31000 standaard daarentegen is nog maar weinig toegepast.

Risicobeheer blijkt nog duidelijk in ontwikkeling en is niet zonder uitdagingen voor de toekomst. De uitdagingen die werden aangegeven door de bedrijven in onze online enquête stemmen overeen met de reeds beschreven challenges uit de literatuurstudie. Bedrijven vinden het moeilijk om een algemene risicocultuur te creëren en deze te implementeren in de bedrijfsstrategie.

Table of contents

List of Abbreviations

BELRIM	Belgian Risk Management Association
CBFA	Commissie voor Bank- ,Financie- en Assurantiewezen
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
FERMA	European Federation of Risk Management
FSMA	Financial Services and Market Authority
IFRIMA	International Federation of Risk and Insurance Managers Associations
IRM	The Institute of Risk Management
ISO	International Organization for Standardization
KPI	Key Performance Indicator
OECD	Organization for Economic Co-operation and Development
PWC	Price Waterhouse Coopers
RCM	Risk Control Matrix
RM	Risk Management
SOX	Sarbanes Oxley
STO	Service Take Out
SWOT-analysis	Strengths, Weaknesses, Opportunities and Threats analysis

List of used figures

Introduction

Risk management is quite a hot topic in the ever changing economic environment. It mainly deals with the identification of risks, how to control them and by doing this, adding maximum sustainable value to all the actions of a business. Any organization should implement risk management because of the many benefits and opportunities that may arise. For instance, it increases the likelihood of potential success, reduces the probability of failure and reduces the uncertainty of achieving objectives. Risk management is a concept that has recently received much attention, but despite this recognition remains insufficiently implemented. This statement can be supported by a report of The Economist (Fall guys - Risk Management in the Frontline, 2010).

Building on this report, before and in the beginning of the financial crisis, risk managers were sometimes seen as people who wanted to prevent the growth. Today, this perception has changed. Financial services companies are strengthening risk departments, making new governance structures, implementing risk committees and, if such a function is present, giving more responsibilities to the Chief Risk Officer. The function of the risk manager has evolved, every manager is looking for peers to exchange experiences with and for benchmarking.

This wave of improving the risk management function does not stop at the banking industry, but goes way beyond. Senior executives are being reminded of the importance of ERM (Enterprise Risk Management) not only by the crisis, but also by accidents of all kinds, the increase of business volatility, growing complexity and extension of business problems. The risk management function helps to deal with all these different kinds of risk.

But, according to the article in The Economist, all of these improvements remain in its infancy stage. Senior executives recognize ERM as important, but this does not show in practice. Proof of this is the lack of significant investments in the risk function. Two reasons for low investments are the ongoing cost constraints and company-wide budget freezes. Another lack in showing interest is demonstrated by the fact that only a minority of companies let risk management play a more prominent role in key business decisions. The article stated that risk managers would like to help managers achieve their business objectives, instead the risk managers are occupied in preventive activities such as controlling and monitoring.

Another concern that is raised is that in spite of the current positive evolution, it is not sure that this influence will be permanent.

Despite of all these comments, there are also some positive signs of change.

Since risk management is still clearly under development, we certainly see the potential for exploring this area in greater depth. We will investigate, in the empirical research part, what the main risks are

that companies come across, who is responsible for managing risks, what companies expect from the risk management function, whether risk management is temporary and which techniques and standards companies mainly use in this area. In order to get these results, we interviewed two companies and executed an on-line enquiry.

In the Literature Review, we will provide the reader with a good understanding of what risk, risk management and Enterprise Risk Management entails. Also, we want to give an introduction of how a standard risk management Process looks like. Techniques for identifying risks are discussed, next to tools and procedures and responsibilities. We also zoom in on the regulatory environment.

Literature Review

In order to evaluate the progress in the area of risk management, we conducted a literature study. In what follows one will find a brief summary of the articles, papers and reports read.

1. Definitions

First of all, some basic concepts, that will occur frequently in the following literature, have to be given some clarity. A definition for risk, risk management and Enterprise Risk management gives an idea of what is meant by these concepts. There are many possible attitudes towards these notions. In this paper there is opted to use an exhaustive definition for all of them.

*'**Risk** can be defined as the combination of the probability of an event and its consequences.'(ISO/IEC Guide 73)* (The Institute of Risk Management, 2002)

A definition of **risk management** is adopted from the Institute of Risk management; they describe the concept as follows:

'Risk management is a central part of any organization's strategic management. It is the process whereby organizations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.' (The Institute of Risk Management, 2002)

The notion of ERM is explained in an executive summary of 'Enterprise Risk Management – Integrated framework' by PricewaterhouseCoopers LLP.

*'**Enterprise Risk Management** is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.'* (Steinberg, Martens, Everson, & Nottingham, 2004)

2. Types of Risks

Now that the most important concepts are identified, a more global overview can be provided. We already know from 'The Risk management Study' from the IRM (The Institute of Risk Management, 2002), that risk management should be implemented into the organization's strategy and should be a continuous process. When integrated in the organization's culture it should contribute to increase the success of the company and reduce also the probability of failure.

In order to integrate risk management properly, one must have an understanding of the different types of risk.

According to the IRM, the risks can be divided into two categories, these are based on **internal and external** drivers. Each category of drivers can on their turn be divided into four groups of risks. The financial, strategic, operational and the hazard risks, this last category is also defined as compliance risks further on. In this paper we will use this classification, knowing that there are other points of view.

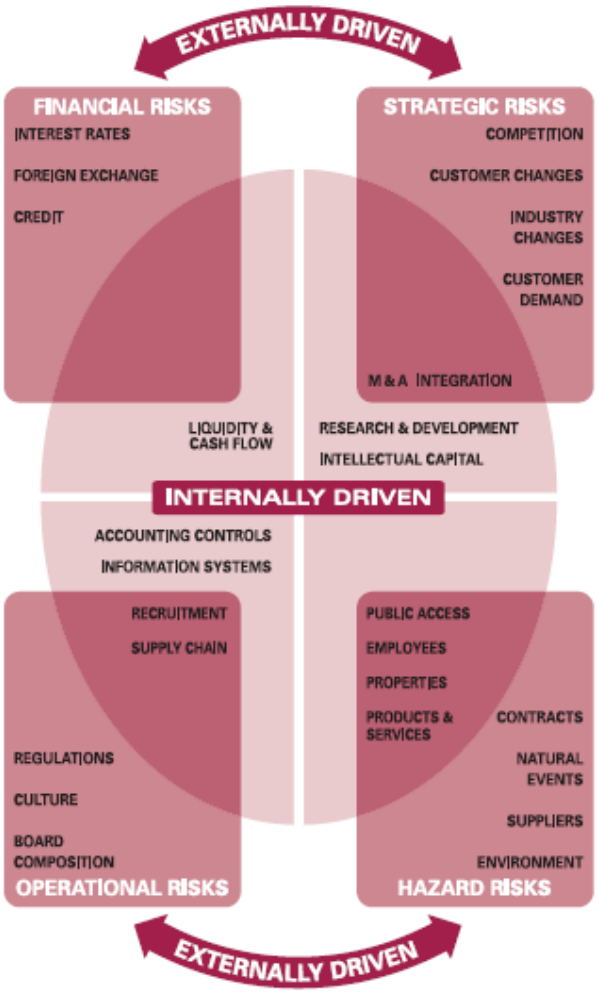


Figure 1. Examples of the drivers of Key Risks (The Institute of Risk Management, 2002)

As one can see from Figure 1, the four categories can be both externally and internally driven. Of course, not all the key risks in a category belong to both the drivers, but only some specific ones like recruitment from the operational risk.

Although there is increasing attention towards risk management, the majority of the companies still does not take into account some major risks in the area of political and image building risks.

Financial risks are perceived as being the most important type of risk. However, organizations should not neglect other types which are also vital to develop a good risk management system. A solution to this, according to Accenture[1], is '*the risk bearing capacity*' (Accenture, 2011) which considers next to the financial risks, the operational risks, the processes and the culture. The '*risk bearing capacity*' comprises five dimensions: financial strength, management capacity, competitive dynamics, operational flexibility and risk management systems. Each dimension is evaluated separately and in interaction with the others.

3. Most important business risks

A study of Ernst&Young has been conducted within 14 global sector groups. The matrix in figure 2, shows that the impact of different risks varies throughout the 14 industries.

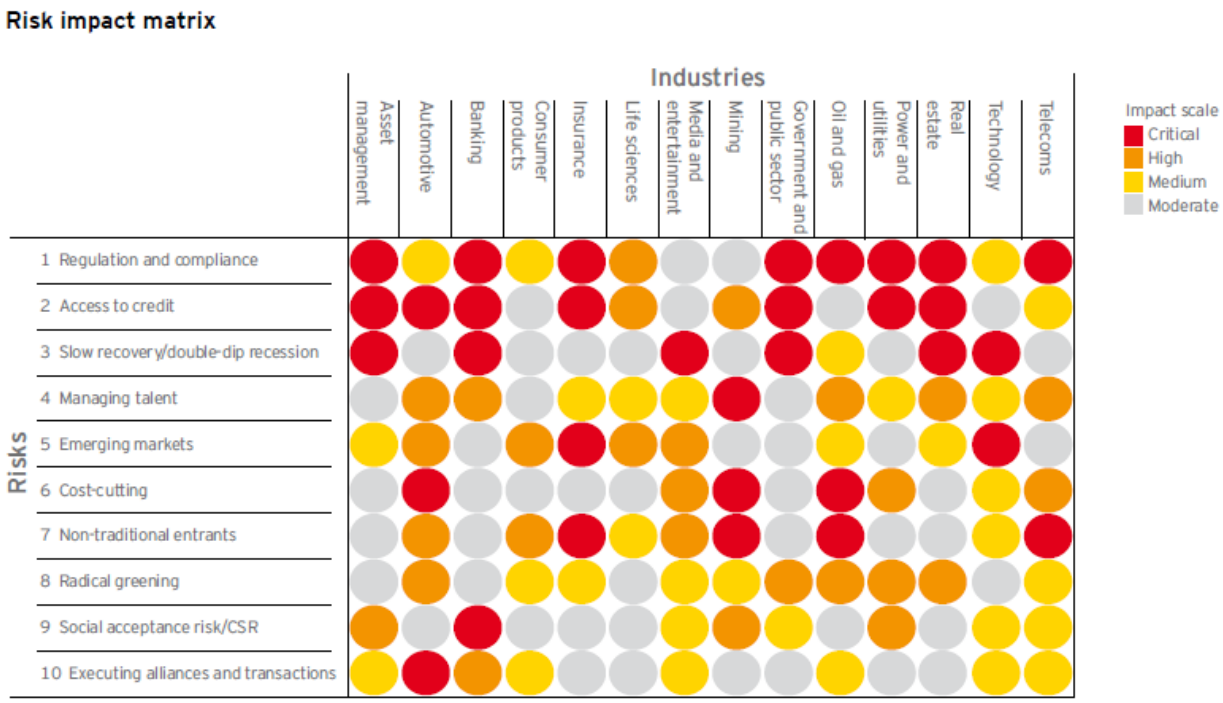


Figure 2. Risk impact matrix (Ernst&Young, 2010)

The most important business risks in 2010 were concentrated in the areas of regulation and compliance - aftermath of the global financial crisis. These risks are represented as a radar (figure 3) and can be divided in the four most important categories of risks according to Ernst&Young, the IRM and this paper.

[1] Accenture considers other types of risk than the IRM, which are also relevant in this context.

- **Strategic**: regulatory and legal changes, customer changes, reputation, competition, capital available
- **Operational**: the day-to-day issues
- **Financial**: the effective management and the control of finance, credit availability, currency exchange rates, interest rates
- **Compliance**: health & safety, environment, consumer protection.

Figure 3. The top 10 business risks (Ernst&Young, 2010)

Ernst&Young also recognizes that the definition of risks varies from sector to sector and from firm to firm, depending on a company's objectives and many other factors.

Compliance threats originate in politics, law, regulation or corporate governance. Financial threats stem from volatility in markets and the real economy. Strategic threats are related to customers, competitors, and investors. Finally, operational threats affect the processes, systems, people and overall value chain of a business.

The most important risks are situated above the radar, these are the 10 biggest business risks:

1. Regulation and compliance
2. Access to credit
3. Slow recovery or double-dip recession
4. Managing talent
5. Emerging markets
6. Cost cutting
7. Non-traditional entrants
8. Radical greening
9. Social acceptance risk and Corporate Social Responsibility (CSR)
10. Executing transactions and alliances

(Ernst&Young, 2010)

4. Risk management Process

After identifying the most important risks and risk categories, a company needs to formally construct their risk management philosophy. This to make clear how risks should be addressed and which attitude towards risk tolerance is appropriate in an entity. Every company should therefore work out a risk management process that contains the most valuable steps of managing risks, so that crucial decisions can be made on the basis of specific guidelines. In our empirical research, we will investigate whether companies have implemented such a risk management process or not.

As stated before, risk should be implemented into the strategy of an organization, so the strategic objectives should be the starting point of the process.

Risk Assessment contains two major subdivisions: **risk analysis and risk evaluation**. This Risk Assessment is influenced by the organization's strategic objectives and is described by the IRM as an overall process.

Furthermore, there are some different steps that can be distinguished within the risk analysis. The most important step is the identification of the different risks, followed by their description and estimation.

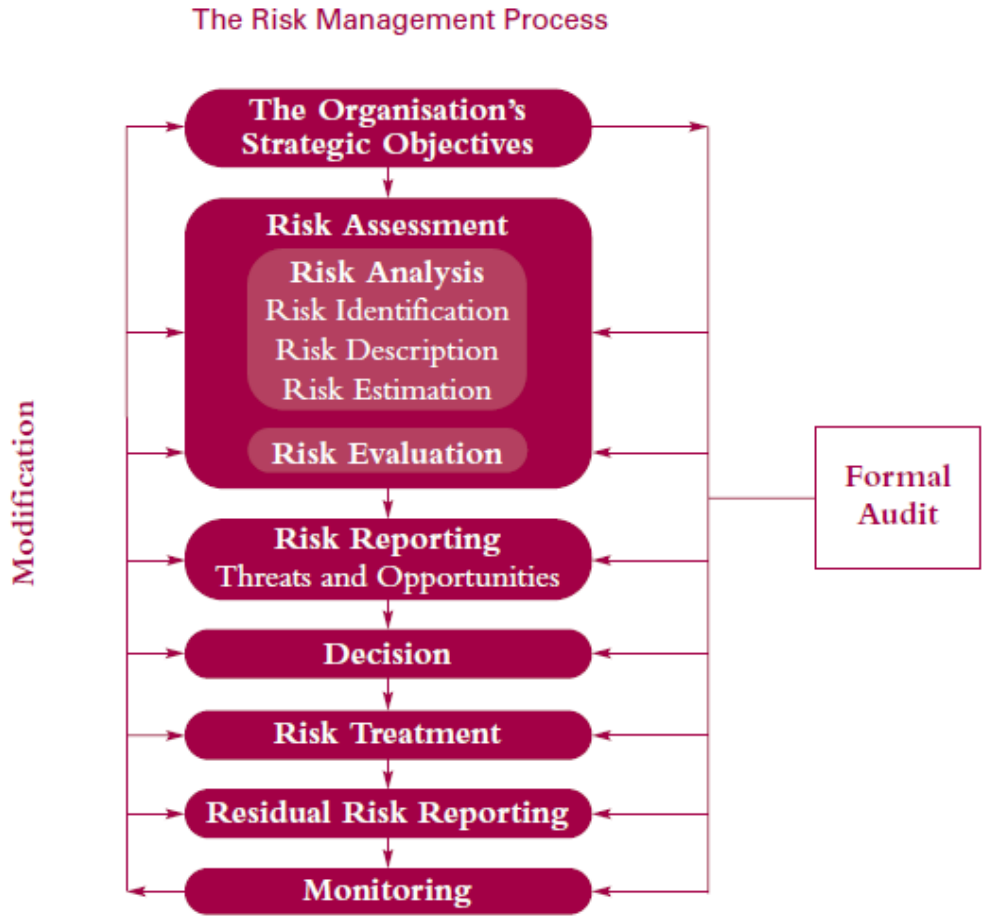


Figure 4. The risk management Process (The Institute of Risk Management, 2002)

Risk identification can be done by external consultants but it is shown that integrating an internal risk management process is likely to be more effective. *''In-house 'ownership' of the risk management process is essential'* (The Institute of Risk Management, 2002). There exist a number of techniques to identify a risk, these can be found under the heading 'Techniques for identifying risks'.

The next step of the risk analysis is to describe the different characteristics of the risk. First of all, the risk has to be classified in one of the four major categories, according to the nature of the risk. Then the scope can be registered. By scope we mean the description of the importance and sequence of the events. Next, the stakeholders and their expectations have an important role in giving weight to the risk. The risk has to be quantified, as in how significant and how high the probability is that the risk will occur, this depends also on the risk tolerance of the company.

How is the risk being treated, or in other words, what are the means that are used to manage it. What actions need to be taken to reduce this risk and who is responsible for working out a strategy to evaluate this. This process is known as the risk estimation.

When the risk analysis process is finished, a **risk evaluation** needs to take place. In this evaluation the estimated risks are compared with the risk criteria created by the organization. These criteria comprise the associated costs and benefits, the regulation, socio-economic and environmental factors, according to the IRM (The Institute of Risk Management, 2002). When these criteria are taken into consideration, a decision about the acceptance or threat of a specific risk can be made.

Risk reporting and **communication** embraces the fact that the result of this risk assessment needs to be communicated. Following the IRM, this reporting of results has to be performed internally and externally. The different parts within the organization have different information needs. For example, the Board of Directors should know which are the most important risks their organization has to deal with. The Business Units' information is limited to the risks that cover their area of responsibility. Employees should be aware of the possible risks and how they can contribute to improve risk management. Externally the company needs to report to its stakeholders so they can evaluate the effectiveness of the organization's policies.

When these results are reported, measures can be implemented to restrict the risks. This can be realized by different controls, like internal controls or by risk avoidance, etc. An internal control determines whether the risk will be reduced or eliminated by the measure that is proposed to be implemented. The risk avoidance level indicates which risks can be tolerated and which ones need to be reduced or eliminated. Important when making this decision, is balancing the costs of the elimination of a certain risk versus the benefits of this elimination. This process is called **risk treatment**.

A last step contains the **monitoring and review** of the risk management process. Systems could need modifications when the operating environment of the organization changes. A review can be performed to check if the risks are assessed and evaluated effectively.

5. Techniques for identifying risks

The Institute of Management Accountants made an overview of the **various** tools and techniques one can use to effectively implement Enterprise Risk Management. (Institute of Management Accountants, 2007) A summary of the most interesting techniques is provided below and the techniques mostly used in practice are provided in our empirical part.

5.1. Brainstorming

A brainstorm session about the possible risks that can occur or threaten a company, can be very useful when the objectives of the session are clearly understood by all participants. Sometimes risks that are never thought off rise to the surface. These sessions ask a well-skilled and talented leader

and all participants of this brainstorming need to understand the ERM framework. A cross-functional team for this sort of tool is very interesting for defining specific risks. The involvement of employees, audit committee and the Board are therefore very useful.

5.2. Event inventories

Event inventories are used to give a basis for the brainstorming session. They give an overview of all the possible risks within an industry. In this session it is the objective to reduce the event inventory to the risks that are relevant for the own organization.

5.3. Interview and self-assessment

Each individual within the organization has to describe the objectives related to their responsibilities. They also have to define the risks that could occur and impede the execution of these objectives. These interviews can be conducted by ERM staff or by the responsible employee of risk management.

5.4. Risk questionnaires and risk surveys

Questionnaires handle questions on both internal risks (customers, suppliers, creditors, etc.) and external risks (political, economic, environmental, etc.). A shorter version of these questionnaires are the risk surveys. These surveys are good substitutes for lengthy questionnaires, completing a survey asks less time and effort of the respondent. Frequently asked questions in this surveys are 'rankings'. The participant then needs to list the most important risks that threaten the accomplishment of the objectives of a company, or he has to rank the effectiveness of management to cope with some specific risks, etc.

5.5. Scenario analysis

Scenario analysis is based on the fact that we cannot predict the future. The only thing we can try to achieve is to determine the different possible outcomes of an event and making an estimation on the probability that such a scenario occurs. After which the responses to every scenario can be conceived next to what the consequences of every scenario might be.

Scenario analysis is especially useful for identifying strategic risks and in a situation which is not well defined. This technique can also be used when an event has a high-impact and low probability. For example, the effects of an earthquake on the activities of the organization. All costs that are related to this event are estimated within the analysis. An event provokes a number of different risks and the accumulation of these risks can have a large impact.

6. Risk assessment tools

An organization can rely on a number of tools to manage risk in a good way. The risk assessment tools can be divided in three categories: the quantitative tools, the quantitative/qualitative tools and the quantitative ones. We provide a brief summary of these instruments.

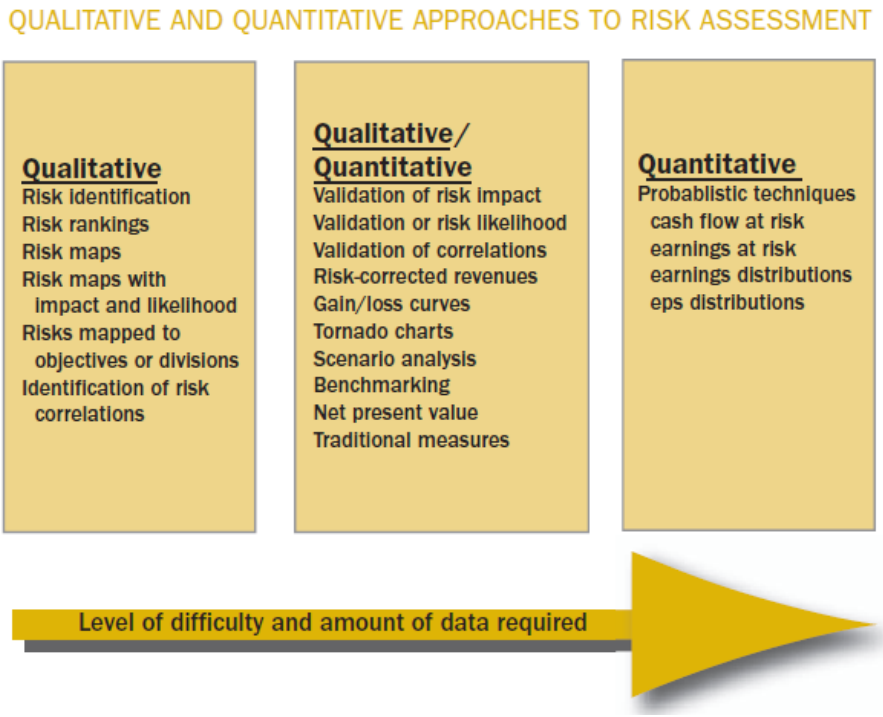


Figure 5. Categories of risk assessment tools (Institute of Management Accountants, 2007)

6.1. Qualitative tools

6.1.1. Risk rankings

When the different risks are identified, these can be ranked on a scale of importance of low, moderate or high. In a cross-functional group, the importance of every risk is discussed because the importance of a risk can be interpreted differently by the members of the group. This discussion group can sometimes lead to a broader understanding and another perspective on some of these risks.

6.1.2. Risk maps and Heat maps

Another commonly reviewed aid to assess risk management are heat maps and risk maps. In the empirical part of our thesis, is investigated whether this attention is deserved.

These are methods to visualize the importance of certain risks. PriceWaterhouseCoopers elaborated the efficiency of this tool in a practical guide (PricewaterhouseCoopers, 2008) on risk assessment. An example of a risk map used by PWC can be found in the appendices, Appendix 1. A risk map gives the advantage to look at every risk individually and in relation with others. First, the likelihood of a risk is

being evaluated, this can be determined as high, medium or low. The likelihood defines the certainty or uncertainty that a specific risk occurs. Furthermore the impact of this risk is being assessed, PWC opted to define this impact in a monetary amount. When every risk is taken into account, the relations and interdependencies between the risks can be evaluated. Some risks that occur together can create a greater overall risk.

When these risks and their relations are assessed, a company can decide on the basis of its risk appetite to deal with these risks. Appendix 2 in the Appendices shows which strategies can be undertaken. Some risks must be accepted, reduced or avoided. The risks with a low likelihood and a low impact are generally accepted by the company. Some risks with a medium evaluation of the two criteria can be reduced by outsourcing or insurance. High impact risks must be avoided, an example of this category are illegal and fraudulent activities.

6.1.3. Executive Risk Dashboard

The next tool we discuss is the Executive Risk Dashboard. In a publication of PWC (PWC, 2010), it was stated that a lot of organizations like to adjust their business model due to the numerous challenges they come across. These challenges range from an unstable and changing climate to new regulation. Companies are reacting to this by implementing risk based controls which should be effective at a strategic and tactical level. However, organizations create often a complex model and a fragmented representation of the risk management approach. A solution for this problem is the creation of an Executive Risk Dashboard. This tool is a customized web-interface that is only accessible by the manager who is authorized to see or manage particular data or information. It provides a dynamic way to see the state of a department or an organization as a whole. This dashboard gives the manager immediate access to information and reports without the otherwise time-consuming actions. In other words, Executive Risk Dashboard serves as a center for risk information, a way for communication and a comprehensive view on risks and visualization.

6.2. Qualitative/quantitative tools

6.2.1. Gain/loss curves

The gain/loss curve gives an insight of how a specific risk can influence and determine the financial result of an organization. When the impact of a risk and its probability is known, the organization can make an estimation about the money that is needed to manage a specific risk. This definition is also supported by the Institute of Management Accountants of which an example of a gain/loss curve is provided below.

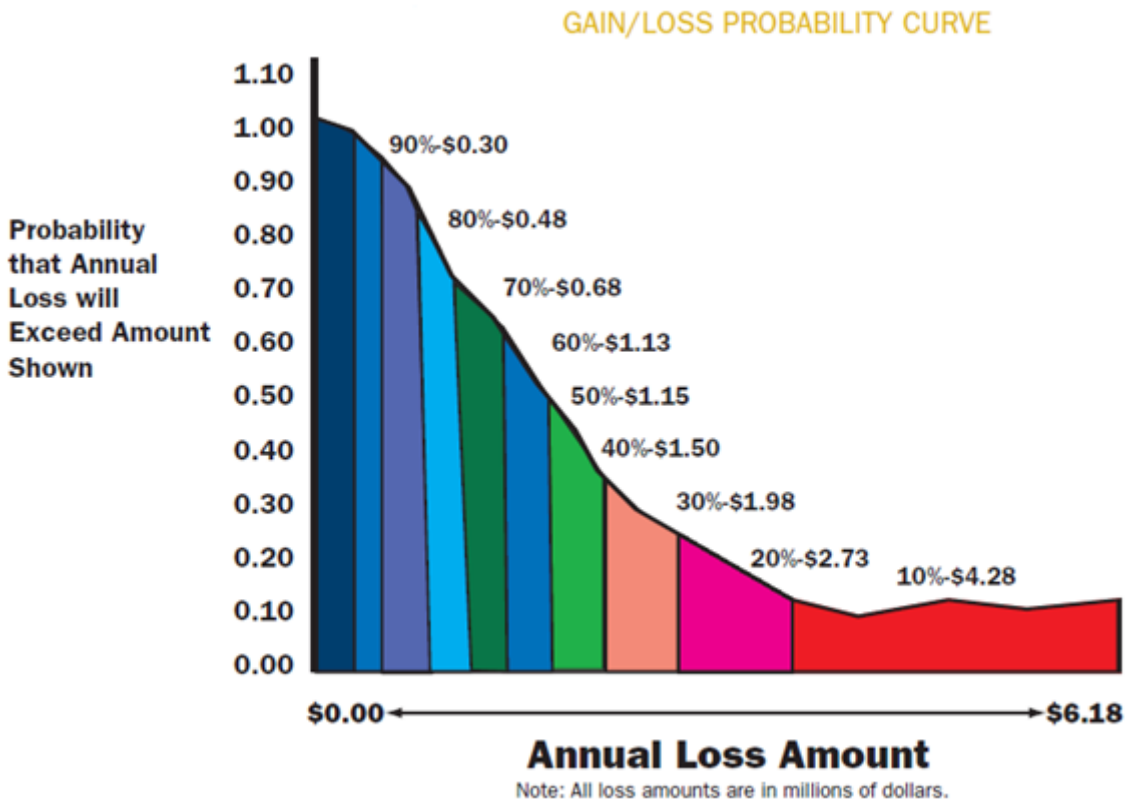


Figure 6. Gain/loss curves (Institute of Management Accountants, 2007)

6.2.2. Tornado charts

A tornado chart shows the impact of a risk on a specific measure like the net income, the earnings per share or the revenues. These are useful for sensitivity analysis which can test the robustness of a study.

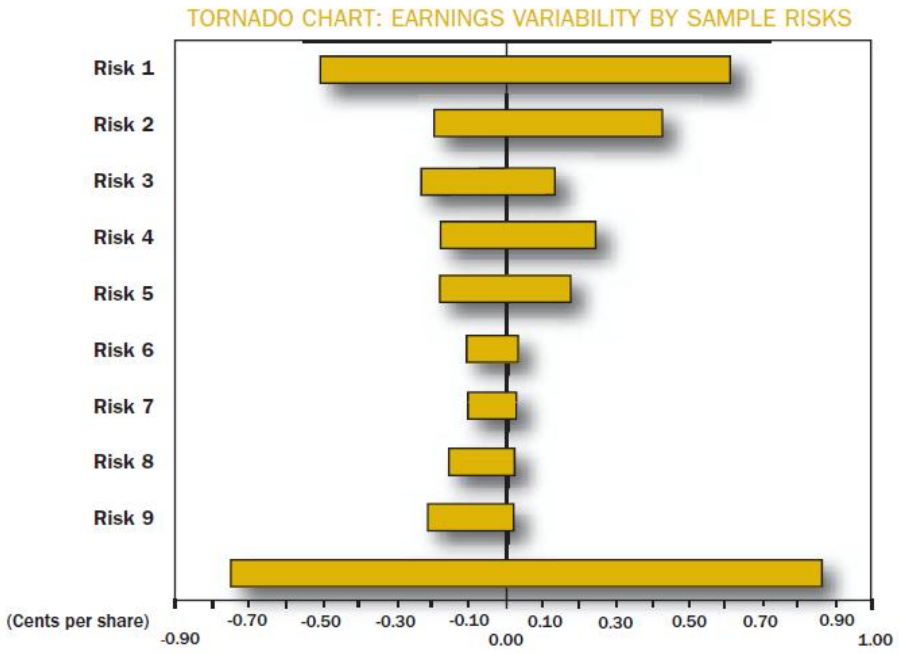


Figure 7. Tornado Chart (Institute of Management Accountants, 2007)

6.3. *Quantitative tools*

Probabilistic and statistical modeling techniques are quantitative ways for evaluating risks. These techniques are not without disadvantages. Making decisions for the future based on the past has its limitations.

7. Organizational responsibilities

We have already discussed how one can do risk management, now we will take a look at who is responsible for ERM. This topic was also put in the questionnaire as a discussion point.

Risk management can be under the responsibility of an executive group, a non-executive committee, and audit committee or another function within the organization. The role of the risk management function knows a different implementation in every entity but the following three tasks are seen as the primary responsibility of the risk function. (The Institute of Risk Management, 2002)

- ~ Setting the strategy for risk management
- ~ Building a culture around risk management, making people within the organization aware of the possible risks
- ~ Designing processes to manage risks and to reduce them

Companies who put more effort in risk management mirror this in the increase of investments in this area and in the number of recruitments of Chief Risk Officers (CRO).

Some companies who decide not to hire a CRO, accomplish this by giving more responsibility to their executives. Risk management can be centralized thus being the responsibility of one person, or the company can divide this responsibility in different business units.

The role of the internal audit in enterprise Risk Management as defined by (The Institute of Risk Management, 2002):

- ~ Auditing the management processes that have been set up to control the risks
- ~ Focusing the internal audit on the significant risks
- ~ Providing support in the management risk processes
- ~ Educating staff in internal control management and helping to identify the different risks

Companies should be careful to use the traditional audit committee for managing risk. Research has been done and it was revealed that the traditional Audit Committee risk management Model is becoming outdated in the complex business situation of today (Brown, Steen, & Foreman, 2009). The Audit Committee becomes overcharged with responsibilities of managing risks. In the same article, it

is suggested that an alternative governance structure is required. This can be the constitution of a risk management sub-committee within the actual Audit Committee or an external risk management specialist or corporate body. The Audit Committee can then focus on their core tasks, which are financial responsibilities and reporting. The operational risks are in this situation managed by the external body or the sub-committee.

8. Regulatory Environment

8.1. External reporting

8.1.1. COSO

A first authority in this area is The Committee of Sponsoring Organizations of the Treadway Commission, known by the acronym COSO. Their mission is *'to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise Risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.'* (COSO, 1985)

To achieve their mission, COSO publishes papers with a lot of useful steps to follow in order to have good risk management. For example, their article about embracing enterprise Risk management (Frigo & Anderson, 2011) contains **7 themes** one has to go through to have a successful ERM adoption. The first theme is the first requirement an organization needs to have, which is support from the top. Next, a company has to take incremental steps meaning that the ERM will not be implemented in one single effort. This also provides the opportunity to a better understanding of the system. Theme three, one has to focus on a small number of priority risks. This is done initially to keep the ERM manageable. Theme five is about leveraging the existing resources, because a company might already have everything and everyone in house, so that big investments are absolutely not necessary. Building on existing risk management activities, which can be done in an organization that already exists. There will always be some kind of risk assessments already in place, e.g. internal audit, compliance functions, etc. Theme 6 deals with the issue to embed ERM in the whole organization in order to be effective. The last theme is about the future, to keep updating the system and to keep educating the directors and senior management.

8.1.2. COSO Framework

COSO developed also the COSO framework in order to help organizations to establish a decent ERM system. The framework consists of three dimensions: four objectives categories, eight components and the entity unit.

The COSO framework sets objectives within four categories: strategic, operations, reporting and compliance. Some objectives can be subdivided into more than one category.
The reporting and compliance category are more easily managed internally because these are based on regulations. The other two, strategic and operations are more dependent on the external environment, as a result these are less easily managed.

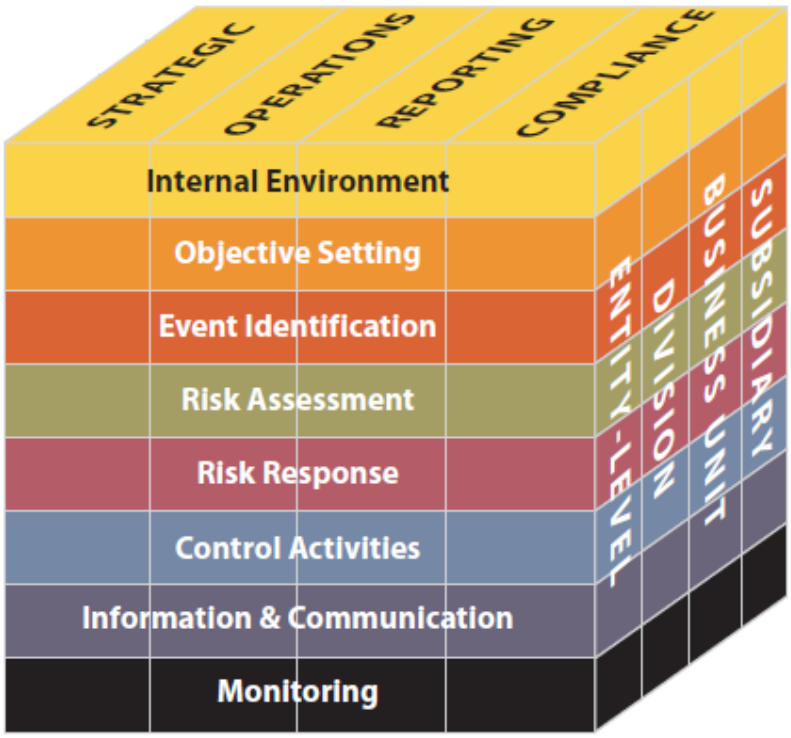


Figure 8. COSO framework (Committee of Sponsoring Organizations of the Treadway Commission, 2004)

COSO gives a definition of the eight interrelated components in 'Enterprise Risk Management — Integrated Framework' (Committee of Sponsoring Organizations of the Treadway Commission, 2004). Below one can find a description of these concepts.

~ Internal Environment – This component tries to develop an overall risk culture. It gives insight in the fact that there are expected and unexpected events that can influence an organization's activities. The internal environment gives guidance for the entity's people because it sets the context in which risks should be evaluated. It gives an idea on the risk philosophy and risk appetite, the integrity and the ethical values that ought to be respected.

~ Objective Setting – Before management can evaluate the events that affect their activities, a straightforward set of objectives needs to be defined. These objectives need to be in line

with the organization's mission and with the level of risk that management is willing to accept. This level consists of the risk appetite and risk tolerance of the entity.

~ Event Identification – Both internal and external events have an influence on the achievement of the company's objectives. Events that have a negative impact are representing risks and events with a positive impact may represent opportunities. Opportunities are passed back to the objective setting and are viewed from management strategy perspective.

~ Risk Assessment – Helps the organization to assess which risks are likely to have an influence on the set of objectives. The risks are identified and analyzed based on two perspectives, likelihood and impact. To accomplish this analysis, both qualitative and quantitative risk assessment tools are used. Further on it assesses these risks on an inherent and residual basis.

~ Risk Response – Management distinguishes and evaluates the possible responses to risks. Risks can be avoided, accepted, reduced or shared. The possible responses are evaluated in the context of the entity's risk appetite, the costs versus the benefits of the several responses and the degree to which a particular response helps to reduce, avoid, accept or share the impact and the likelihood of the risk.

~ Control Activities – These activities should ensure that the risk responses and the other company directives are performed effectively. The control activities are the procedures and policies that are established to obtain a perfect execution of the predefined tasks. These activities are implemented throughout the whole entity, at every level and in all functions.

~ Information and Communication – To effectively perform their responsibilities, all people in the entity should have access to the most relevant and recent information. Therefore all useable information is identified, captured and communicated in a form and timeframe that facilitates employees to fulfill their tasks. The communication happens in a broad sense, top-down, across different company levels and upwards in the organization.

~ Monitoring – This entails the evaluation of the effectiveness of the process and determines how well the Enterprise Risk Management is executed. The company should decide on minimum standards on every component so that performance on each concept can be evaluated objectively. Monitoring can be done in two ways, through ongoing management activities and via separate evaluations.

All of this can be applied on different levels, which is also defined by the COSO as the third dimension. This dimension consists of the subsidiary level, the business unit level, the division level and the entity-level.

8.1.3. ISO 31000

Another authority that covers this topic is the International Organization for Standardization. This organization publishes international standards and more importantly, some of these relate to risk management standards. ISO 31000, published in 2009, wants to answer what risk management is about, its implementation and the possible achievement. (Airmic, Alarm, & IRM, 2010)

ISO 31000 is a framework for implementing risk management and not a framework for supporting the risk management process. For the latter one should use the risk management process, supra *4. Risk management Process*. ISO 31000 consists of 5 components with Mandate and commitment by the board being the first one. This is followed by Design of framework, Implement risk management, Monitor and Review framework and Improve framework. (Airmic, Alarm, & IRM, 2010) Important to note: it is applicable for all organizations who are concerned with risk management.

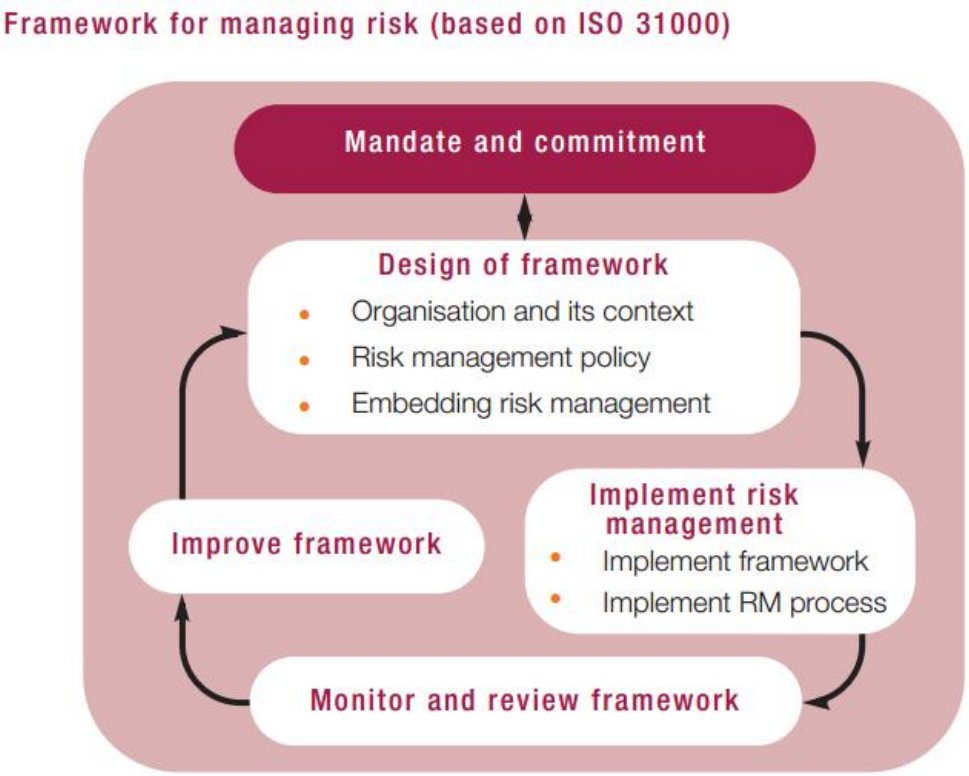


Figure 9. Framework based on ISO 31000 (Airmic, Alarm, & IRM, 2010)

8.1.4. Belgian Law of April 6, 2011

On April 6, 2011 a new requirement was introduced to meet the terms with respect to the internal control and risk management systems. Listed companies are now obliged to mention their main features in the annual report. In this manner an attempt is made to a clearer understanding of the corporate governance of the company, and more specifically of the internal control and risk management systems. In our empirical research, we will investigate, next to COSO and ISO 31000, if this new law has had an impact on the risk management in organizations. The Corporate Governance Committee has worked out some guidelines to simplify these requirements.

The Financial Services and Markets Authority (in Belgium used to be known as 'CBFA' [2]) conducted a survey at the end of 2010, regarding the compliance of the new directions concerning the disclosure requirements imposed by the Belgian Corporate Governance Code 2009. It was revealed that, based on the annual financial reports of listed companies, certain provisions were not respected. These provisions are primarily related to internal control and risk management system, evaluation of directors and the procedure concerning the remuneration policy.

The Corporate Governance Committee has worked out some guidelines for listed companies and small enterprises to simplify the requirements of the law of April 6, 2011 and to comply with the recommendations of the Belgian Corporate Governance Code 2009.

The directives envisage two purposes:

"*1. To form a basis for compliance with the legal obligation to describe the main features of the internal control and risk management systems, associated with the process of financial reporting in annual reports of listed companies. To this end, these guidelines are supplemented by a questionnaire.*

2. To form a basis for compliance with the legal obligation of the 'comply or explain' principle of the 2009 Code provisions on internal control and risk management. For this purpose, a questionnaire is completed by these guidelines." (Commissie Corporate Governance, 2011)

[2] On April 1, 2011, the 'CBFA' changed its name to 'FSMA', Financial Services and Markets Authority, due to its changed mission. "The FSMA is responsible for supervising financial markets and listed companies, the approval and supervision of certain categories of financial institutions, the rules of conduct by financial intermediaries and the commercialization of investment products for the general public and the so-called social control on supplementary pensions. The legislature has also imposed the FSMA a contribution to the financial formation of savers and investors." (Financial Services and Markets Authority)

The questionnaires which were drawn, serve as a basis for every company and can be further adjusted according to the specific characteristics of the enterprise.

The first questionnaire deals with the first aim that is described above. This questionnaire addresses five topics, i.e. the control environment, risk management, control activities, information and communication and adjustment. The control environment poses questions about who is responsible for the accounting and financial function and whether rules were established in this area. Risk management deals with questions about compliance with the law, risk identification and analysis and similar issues. The control activity is about how control is organized and whether there are control procedures. Information and communication covers questions about what procedures and systems exist in the company, if there is a chance of feedback, are there relationships with IT service providers, and so on. The last topic, adjustment, mainly deals with questions relating to the adequate informing of the governing body.

The second questionnaire covers the same topics, but more detailed. According to the Corporate Governance Committee, the internal control and risk management process belongs to the task area of the administrative body, the audit committee, the commissioner, the executive management and the internal audit.

8.2. Corporate Governance

In order to control risk in a proper way, we also need to take a closer look at corporate governance. As Alnoor Bhimani states: "*Risk can be managed by better appreciating the value of institutional corporate governance practices vis-à-vis those at the country level.*" (Bhimani, 2009)

8.2.1. Definition

We will use a definition of Corporate Governance from the OECD throughout this paper, knowing there are other definitions.

'Procedures and processes according to which an organization is directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among the different participants in the organization – such as the board, managers, shareholders and other stakeholders – and lays down the rules and procedures for decision-making.' (OECD, 2005)

8.2.2. Corporate Governance as a tool

Corporate Governance is essentially a tool that makes managers more accountable to shareholders. This tool is a social construct that is shaped by the context in which organizations operate, meaning there can be differences across countries and perhaps across companies.

According to Alnoor Bhimani (Bhimani, 2009), there are a number of terms linked with Corporate Governance such as disclosure, economy, effectiveness and efficiency. However, the two most important concepts are **transparency and accountability**, the term accountability does not need more explanation, transparency does. Today, it is not sufficient for companies to only implement corporate governance, but they also need to make their commitment transparent. This transparency is needed in order to sustain their legitimacy. Out of this, we can conclude that corporate governance also influences the value of a company.

8.2.3. Board of Directors

Recently, a part of risk management is added to the responsibility of the Board of Directors. The role of this Board should be extended with the task of giving an overview of risk management policies, practices and performance. According to Brown et al, 2009, the Board must also elaborate Corporate Governance systems which provide accountability and which are aligned with the risks involved. On the other hand, the Board is not responsible for managing these risks, but management is.

8.2.4. European Corporate Governance Code

The European Commission decided not to implement a European Corporate Governance Code. "*The Commission does not believe that a European Corporate Governance Code would offer significant added value but would simply add an additional layer between international principles and national codes."* (DG Internal Market, 2003). Listed European Union companies should have a corporate governance statement, this statement includes the code a company decided to apply and the provisions with which it does not comply.

9. Challenges for future risk management

From Accenture (Accenture, 2011) we derived some challenges for future risk management.

- ~ In general, one can state that risk management needs to have an important part in the management of volatility in the economic and financial environment and in the increasing complexity of the organization.
- ~ One must pay more attention to risk management particularly in areas like regulation, competition, customer expectations, technology, etc.
- ~ Becoming risk master to create a competitive advantage. Some enterprises are masters in managing business risks. They create shareholder value through risk management, involve risk organization in decision-making and implement risk awareness in their culture. These companies have a head start at the level of risk capabilities and try to gain competitive advantage from this.

10. Summary of the literature study

From the literature review we can draw some conclusions. We now know that there are many interpretations of the concepts 'risk', 'risk management' and 'Enterprise Risk Management'. As a result, we had to choose one definition for every concept in this paper in order to avoid confusion, so we relied on the definitions of the IRM and COSO.

There are a lot of different risks, which differ from organization to organization and from industry to industry. In order to overcome this and gain in understanding, we divided these different types of risk into four categories, the financial, strategic, operational and compliance risk. This division made it also easier to see where the most important business risks are situated; in 2010 these were located in the compliance area.

We also noted that there exists a basis for the risk management process. Every organization should go through at least one or all steps in this process. Important to say is that this should always be adjusted to the organization, because every organization is different. One of the first steps is the identification of risks. In order to do this properly, a company can use certain techniques like, brainstorming, event inventories, interview and self-assessment, scenario analysis and risk questionnaires and risk surveys.

After the identification, a company can rely on some tools and procedures to manage risk in a good way. These tools can be classified in three categories: the pure qualitative, pure quantitative and quantitative/qualitative category. In the first class of tools, we have seen some interesting procedures like *heat maps* which are a commonly used aid to visualize the importance of certain risks. A great advantage of heat maps is that it gives the user the opportunity to look at every risk individually and in relation with others because some risks that occur together can create a greater overall risk. Other tools in this category are risk rankings and the executive risk dashboard. In the pure quantitative class are *probabilistic and statistical techniques* available which are, as stated, not without disadvantages. In the mixed category we have briefly discussed *gain/loss curves and tornado charts* which are both visual techniques.

Also important to note is, who is responsible for risk management. We can conclude that this can differ between an executive group, the financial department, the audit committee and the chief risk officer.

The risk management concept is gradually becoming more regulated, the Belgian law of April 6, 2011 is proof of this. But before this, we already have The Committee of Sponsoring Organizations making frameworks to facilitate the establishment of a decent Enterprise Risk Management system. This

framework consists of four objectives, eight components and the entity unit and is worldwide used. Next to COSO we have the International Organization for Standardization who published some standards related to risk management.

Besides the regulatory environment, we also saw that corporate governance is important in the context of risk management. This is basically a social construct to make managers more accountable. The implementation of corporate governance can be different across countries and even companies.

With all this knowledge in mind, we can now move into the empirical section of this paper.

Empirical research

We start our empirical research with two case studies that we have performed in two Belgian corporations. For confidentiality reasons, we cannot name the two companies. In these two companies, we have had interviews with the responsible persons concerning risk management. The questions we asked them can be found in the 'Appendix', Appendix 3. As is usual with the application of interviews, we used the proposed questions as a '*scenario of a conversation*' (De Pelsmacker & Van Kenhove, 2010). Based on these questions, we tried to discuss in more depth the proposed subjects, using the technique of probing[3].

The first company is active on the printers and managed document services market. The enterprise has a headcount between 500 and 1000 employees. As to the turnover we can say that it is a company that is situated in the largest group of our survey: between € 151 - 300 million. Our findings of this company are presented in 'Case study 1'.

The second company is active in the steel industry. The headcount is situated in the highest group of our enquiry, the Belgian locations together employ more than 1000 employees. Concerning the turnover, the European segments generate revenues that can be classified in the category of 1001-2000 million Euros. The findings of this organization can be found in 'Case study 2'.

In this first part, we will explore the theory compared to practice within this company.

We also conducted a generic survey to look into the risk management of companies in Belgium. In the second part of our empirical research, we will provide the reader with our findings.

Case study 1

The first company[4], which offered us the opportunity to look into their risk management in depth, first informed us on their risk management process. Exactly as we read in the specific literature, this company has worked out a step based process which we will clarify below. This process was explained to us by the Risk Manager and Compliance Expert. Afterwards, more information about risk management is provided by the internal auditor.

1. Risk Management Process

The company opted to design a Risk Management Process that is implemented in all its affiliates around the world. In this way, a uniform Risk Assessment can be realized. All risks are measured and tackled in the same way, which gives rise to the application of best practices. This also answers the question where risk management is originated in this company. Although the audit and risk

[3] Stimulating of answers (De Pelsmacker & Van Kenhove, 2010)
[4] Active on the printers and managed document service market.

department is very keen on doing risk management, it is imposed by the corporate level of the group.

The process is composed of six sequential steps: the Information Security Measures Baseline Gaps, the Department Information Asset Register, the Risk Assessment, the Risk Treatment Plan, the Risk Acceptance Form and the Risk Register. Step 4, 5 and 6 have not been conducted in the past and are in full development.

It is important to notice that the people who are responsible to help with the mapping process of all the possible risks in this company, are trained in risk management. In that manner, the company knows that risk management will be done is the best possible way.

1.1. The Information Security Measures Baseline Gaps

The first step they take to manage risk is the IS Measures Baseline Gaps. This concerns a number of policies needed to reach the ISO 27001 norm. The company keeps track of the status of these policies in an excel sheet. In this excel sheet one can find different tabs which stand for the different assets like hardware, software, etc. In these tabs there are a number of columns with inter alia the different policies and their status. With status is meant that the company, or more correctly, the departments gives a specific policy a specific label. To make this more concrete, we will give an example.

We see in the tab 'Services – Buildings' (which is the asset), a row about 'Entrance and exit authorization of visitors' (policy). In this row we can find an explanation of the policy and if the control is fully implemented, mostly implemented or partially implemented (status).
When we arrived at our appointment in the company, we needed to register ourselves at the reception and received a badge to enter the building. With this badge, we could only enter certain rooms. We could not enter, e.g. the Human Resources department because they handle confidential documents. So, the policy of 'Entrance and exit authorization of visitors' is in place, as a result the status of this will be 'the control is fully implemented'.

This labeling happens for every asset and policy in the company. Moreover, they do not only look at their own findings, but the company also compares itself with the organization in London. London is the company's baseline, they always need to perform equally or do even better than London, this can be seen as a form of benchmarking.

In order to make an overview of how well the company is performing and to display the comparison with London, they have made an interactive 'Baseline Objective Summary'. This is a radar chart

where the current situation from their company and the offices in London is presented with the possibility to denote an ideal level of compliance. For an example of the chart, see Appendices 4 a&b.

1.2. The Department Information Asset Register

The next step is about registering assets. The company has four broad categories: hardware, software, people and information.

Again, they make use of an excel file to list all of the department's critical assets. The departments also assign three criteria to assess the assets subcategories. The three criteria are confidentiality, integrity (is everything correct) and availability. These criteria can all be rated as high, medium or low and also receive a color code. If there are bars in the color, then they are performing at the same level as London or even better. In other words, they use again benchmarking with London. The establishment of this color code is done in the next step.

Depending on the color, they look into the possible risks associated with the asset's subcategory, e.g. PC's for hardware, in more detail. Green, orange and red are used, with red being the color where the possibility of a risk is the highest. This should not be confused with the ratings on the three criteria. If an asset scores high on confidentiality, this does not mean that this will get a red color. The same for example with low availability, this could be green if there is only a low probability of risk involved. This could be red for another asset if the probability of a risk occurring is high.

1.3. The Risk Assessment

After identifying all critical assets and their possible risks, the company will take action to reduce the impact of the possible risks. However, before the company treats the risks, it has to decide which ones will be put aside. In order to do this, all risks get a color in this step.

In order to get the color-code, which we have already mentioned, the company uses a specific methodology which is presented below.

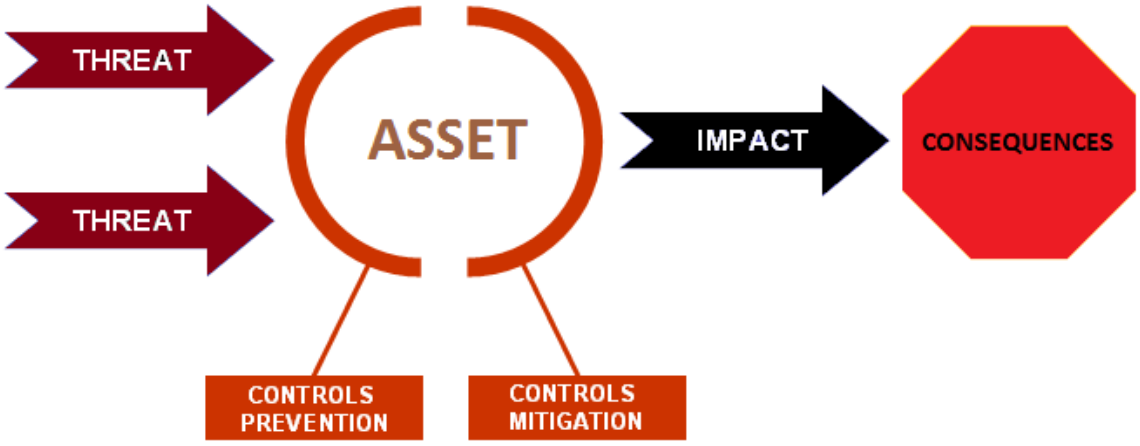


Figure 10. Risk assessment methodology

Depending on the possible threats and the asset, the company calculates the impact and the probability of the occurrence of the risk. The probability depends on what controls exist related to prevention and mitigation.

The impact and probability are both rated on a scale from one to sixteen, one being, respectively, 'no perceived impact' and 'very unlikely', sixteen on the other hand is 'catastrophic impact' and 'happening', respectively. Then both dimensions are being multiplied in order to get a value they can compare with the risk threshold values. The risk threshold values are three numbers which are determined in advance: four, fifteen, thirty-one.

GREEN	Lower than 4: Risks are being accepted, without interference of management.
ORANGE	Between 4 and 15: Risks are accepted, after review from management.
RED	Between 15 and 31: Risks require consideration, but management discretion is allowed.
RED	Higher than 31: Risks require immediate consideration.

The color-code RED means they go on to the next step, ORANGE and GREEN means there will be a form signed by the management for accepting the risks. This process can be compared to the Heat map tool.

		E	D	C	B	A
		1	2	4	8	16
Very unlikely	1	1	2	4	8	16
Unlikely	2	2	4	8	16	32
Feasible	4	4	8	16	32	64
Imminent	8	8	16	32	64	128
Happening	16	16	32	64	128	256

Figure 11. Heat map

As mentioned, the next steps are not yet implemented, but the preparatory steps have already been made.

1.4. The risk treatment plan

In this section of the risk management process, the company introduces possible risk treatment options. Afterwards they will compare the risk rating before and the risk rating after the treatment. They also estimate the cost related to the proposed solution so the organization can perform a cost-benefit analysis. Depending on this analysis, the company decides to go through with the

remediation or not. They will proceed in the case where the benefits of lower risk rating, are higher than the costs. In the other case, where the costs are larger than the perceived benefits, the company will accept the existence of the risk in a risk acceptance form. This creates the next step in the process.

1.5. The risk acceptance form

This section of the process is the result of all the previous steps where the enterprise has listed all the assets and their associated risks.

The acceptance form will be filled out in two occurrences. The first one is when the asset has a green or orange color on all three criteria[5] in the 'department information asset register' step. In this case, the company will go straight from step three to this one. The other case will occur when the company has looked at treatments, but the costs were higher than the benefits.

The form is divided in three parts. The first contains the name of the asset, a description of the asset and the business impact analysis. The latter one consists just of the three criteria of confidentiality, integrity and availability. The second part deals with the threat (risk), the vulnerability (possibility of the occurrence of the risk) and the policy reference (first step). In the third part, one has to complete why the company will not implement a control or policy, how long this acceptance form is valid (from one week to a year to indefinitely) and who is accepting the risk.

1.6. The risk register

This final step is one of summarizing all the risks the company came across. Again, they use an excel sheet to list the risks. Some examples of what they will be listing are risk ID, the date the risk was registered, the likelihood of the risk occurring, early warning mechanisms and when the next review date will be.

The subsequent information serves to get some insights in the internal control environment. The following topics are being discussed: the Business Workflow Diagram, the Risk Control Matrix, the SOX test and the Reporting of the results of these tests. These are all SOX requirements and they are being evaluated on a regular basis.

2. Business Workflow Diagram

The organization makes use of flowcharts to shape it's processes. A flowchart gives insight in the operation's flow of the business process and helps to understand the risks and controls that follow from the operation's work flow. It shows a schematic representation of how a certain process is

[5] confidentiality, integrity and availability

designed and can indicate whether a certain control is effective or not. Further on, it is a tool to identify and help standardize operations. The organization uses these flowcharts not only for identifying risks but also for reviewing the other internal control purposes.

3. Risk Control Matrix

A Risk Control Matrix (RCM) is a risk framework to manage internal control. It's main objectives are:

- ~ The evaluation of the design effectiveness of the internal control system to check if every relevant control to address risk is being implemented. All the controls that are identified with the RCM should be subject to this evaluation test of design effectiveness.
- ~ The Risk Control Matrix is a representation of the above mentioned evaluation process and provides the necessary information on which the evaluation of design effectiveness is based. The RCM consists of the following items: identifying the process objective and assertion linked to risks and controls, identifying risks that impede the achievement of internal control objectives, identifying controls to reduce risks, identifying the department and the people who are responsible to execute the controls and finally, the conclusion on the design and the effectiveness of the internal control.
- ~ The RCM evaluates the significance of the effectiveness of a certain control. If a control is not working at the required level, then they derive what the risks associated with this lack of effectiveness are and how this deficiency should be addressed.

The following figure shows the relationship between the assertions of a process objective, the risks and the controls.

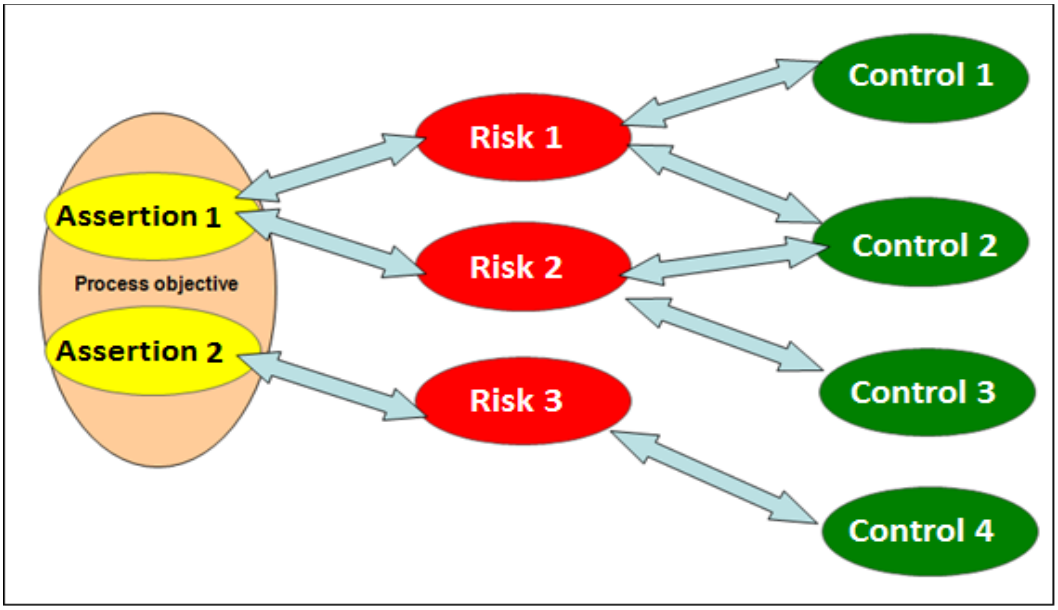


Figure 12. The relationship of assertions, risks and controls

3.1. Process Objective

As an example, we take the purchase process, with the sub-process of inspection and acceptance. The process objective defines which process should be executed. Within the purchase process this means that all purchase requests that are made, should be authorized, documented and approved by the responsible level of management. A process control objective is aimed at achieving a specific process objective. Whenever a process has different process control objectives, the process has also different assertions.

3.2. Assertions

A process objective contains several relevant assertions, also called internal control objectives. These assertions are required for the preparation of a correct financial report and are crucial for constructing an internal control system.

There are different internal control objectives (or assertions) that can be applied.

- *Existence or occurrence* - this means that the assets, liabilities and ownership must exist at a specific cutoff date. The transaction must have taken place during the indicated period.
- *Completeness* -all assets, liabilities and transactions must be booked during the appropriate period.
- *Valuation or allocation* - all assets and liabilities must be booked at the proper value according to the rules of the different relevant accounting standards and procedures.
- *Presentation and disclosure* - each item in the financial report should be presented, described and classified as appropriate.
- *Rights and obligations* - all assets and liabilities that are stated in the Balance Sheet on a certain date must be within the ownership of the company.

The company that we interviewed added two additional internal control objectives to the five listed above.

- *Safeguard of assets* - the assets must be protected from being lost, wasted, used inefficiently or misused. This is the main purpose of this assertion.
- *Prevention of fraud* - the establishment of systems that prevent the possibility to commit fraud. Management and employees should comply with the law.

3.3. Risk

There exist two types of groups that are conceived as risks: the factors that prevent the achievement of the process objectives and factors that impede the achievement of assertions.

First of all it is important to grasp the factors that are conceived as risks. Whenever a transaction takes place, risks have to be taken into account. It is not because there are controls in its place to mitigate certain factors, that every risk is effectively controlled. Further on, the risk level has to be set, this was already mentioned in the second step of the risk management process. When the risks are assessed these can be seen in relation to the assertions. Finally, one can determine which assertions are affected by which risk.

3.4. Control

A control is a system, a procedure and a policy, that is in place to reduce risks. Controls can be divided into four classes according to the preference for reliability and desirability. Controls can be split into human and automated controls. By using human controls, the tasks are mainly performed by one group of individuals. Automated controls are executed by an IT system or a program application. The control can also be preventive or detective. Preventive controls are designed to prevent the appearance of certain errors and are usually applied where risks might be generated in the process. Detective controls on the other hand are designed to detect the errors so that they can be solved.

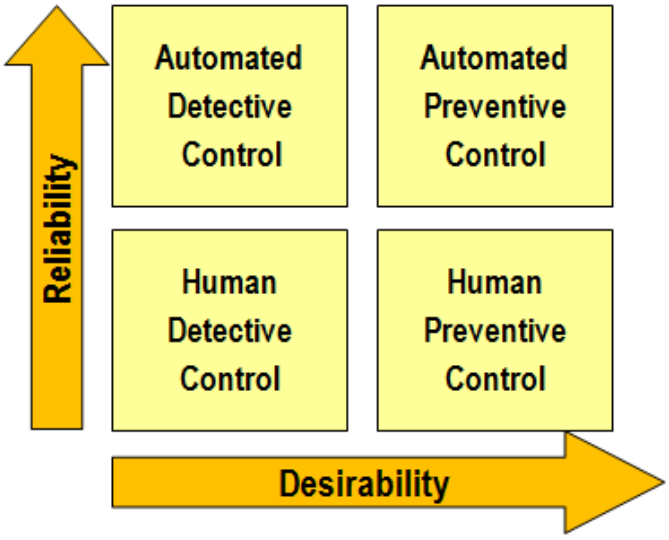


Figure 13. The relationship between reliability and desirability of a control

A delicate balancing between the strictness of the risk control and the cost according to the system is needed.

3.4.1 Type of controls

~ *Review/Approval* - The tasks that people perform within their function can be reviewed by the supervisor or manager. It can be that the work of employees needs to be approved by an authorized person, normally the supervisor or the manager. But this can also be done by a third party. An example of a task where review or approval is in its place is when an order is processed. All the contracts that are handled by the Contract and Support department are being controlled by an employee of the Controlling and Financing department. Checks on correctness, completeness and to prevent fraud are being performed.

~ *Mapping of the system configuration/Mapping of the account title* - Some types of transactions are automatically booked via an automated journal entry. This system prevents that straightforward orders are booked or processed incorrectly. In the example of the processed order this comes down to the fact that an incomplete order cannot be processed by the accounting system in UNIX (the operating system). Due to this lack of data, a delivery of the order is impossible.

~ *Report of exceptional or abnormal items* - The exceptional or abnormal facts need to be reported to the manager or supervisor. Special items in the order processing are Service Take Outs (STO's). When a company delivers a service, service expenses belonging to a specific contract need to be taken into account.

~ *Interface/Data exchange* - It is important that the exchanged data is controlled on their correctness and consistency. This type of control tries to optimize these data exchanges.

~ *Key Performance Indicator* - By setting a KPI, one can evaluate if the targeted level of achievement is reached.

~ *Reconciliation and adjustment* - The reports of the processed information are checked on the occurrence of errors or fraud. The employee of the Contract and Support department needs to verify whether the physical contract that is signed by the customer is in line with a required checklist dossier form. This is done for every new contract to be sure that the processed data is accurate, that the correct contract is used and that the Service Take Out is checked.

~ *Access control to system, information and assets* - Someone who is not authorized to view or get certain information should not be able to get access to these data. Information files are therefore protected and the access to in-out records of the computer room is also restricted.

~ *Job segregation/Mutual control* - Also called segregation of duties. It cannot be allowed that someone is authorized to evaluate and approve his own work. A segregation of duties exists between the department who enters the order in the accounting system and the department that releases the order.

3.5. COSO components

The interviewed company uses the COSO Framework as a tool to evaluate the effectiveness of the internal control over financial reporting. All the applied controls need to be classified in the appropriate section of COSO's internal control framework. Instead of using the eight components framework as described in our literature part of this thesis, the organization uses the five components framework.

The Control Activity is seen as the most important component, it covers all the policies and procedures to achieve the control objectives, all these activities should be taken at the corporate level. The second major component concerns the Monitoring. The quality and the functionality of the internal control system is monitored on a continuous basis.

The remaining three components are seen as equally important. The Control Environment deals with the quality of the members within the organization, more specific with their integrity, ethical virtue and the human aspects of capacity, and with the environment in which the process is carried out. The final two elements are the Risk Assessment and Communication. The Risk Assessment serves to analyze all the risks that could impede the accomplishment of the organizational objectives. It also helps to determine the risk management policy and it is a system that corresponds to environmental changes and renewed risks.

An example that shows how all the above explained concepts are implemented in a Purchase Order process, can be found in the Appendices, Appendix 5.

4. SOX - test

All the processes that are in place should be tested on their accuracy. These tests are performed on a monthly basis by the so called SOX testers. To illustrate the function of these tests, we will explain how the processing of an order is controlled.

To ensure that all orders are prepared and calculated accurately and completely, there should be segregation of duties. So the employee who processed the order never releases the order for delivery. All processed orders are checked by a different employee of the administration department

and for all finance contracts a credit check needs to be conducted. The purpose of the SOX test is to assess if all these controls are preformed and documented correctly.

5. SOX - test results

The results of the previous mentioned tests are reported per entity. The test ID is indicated, this is the tested control process, the test frequency and the overall judgment. The overall judgment shows whether the test is executed and whether the test has passed or failed.

6. Responsibilities concerning risk management

In each department there is a dedicated person for identifying the specific critical assets of his department. This identification of these assets forms the input of the Asset Register in the second step of the Risk Management Process. Each department is therefore informed on the usefulness of this asset registration and on the usefulness of identifying risks.

Further, there are different persons who are responsible for the controls to mitigate or eliminate certain risks. There are operational employees who perform certain controls on a daily, weekly or monthly basis. Next there are supervisors, managers and directors who are authorized to perform controls periodically. As mentioned before there are the SOX testers, who perform tests on a monthly basis and also the Internal Auditor performs a monthly audit.

Case study 2

The second interview was conducted in a multinational organisation which headquarter is situated in Belgium. Its activities are situated in the metal industry and their products are being used in several sectors. The topics handled below give an indication of the conception of risk management in this organisation. We provided a description of the internal control, the ERM process, the responsibilities, the driving force for risk management and the role of consultants. This information was provided to us by the Internal Auditor and Risk Manager.

Risk Management in this company comes down to one major question, 'How to keep it sustainable?'. When an investigation concerning risk management is conducted, there should be no surprises. Each manager needs to know everything about his projects, departments, and more specifically, his risks. Management is the owner, the responsible person, so there is no chance of passing the blame. The general rule is that they do not benchmark against other companies, the internal management needs to know what they are doing and why they are performing certain activities or how to handle some specific risks.

1. Internal Control

Everyone, from the top to the bottom of the organization, needs to be involved in the internal control. It is more or less incorporated in their job description. On the other hand internal control is not something that is tangible; it cannot be exactly pointed out.

First of all, internal control is about keeping the assets in a good shape. The ones that are still in the company need to be maintained, for the ones that leave the company, one needs to make sure that they do not disappear in an uncontrolled manner. The core concept is doing business in an efficient and effective way.

Further on, there are some procedures and rules in place, in order to prevent people from making mistakes. This can be clarified with an example with regards to the accounting system: this is now handled by software, so one cannot make mistakes concerning the balancing between active and passive or debit and credit. Most of the transactions have a standard booking that is known by the software and described in accounting manuals that can be consulted by the employees. Since this organization is not only operating in Belgium, the other affiliates are using the same software to obtain a uniform representation of the financial results.

Finally, there are also systems that need to prevent fraud. However, when two staff members conspire, the systems can be bypassed and these controls on fraud will fail. This event of fraud is called collusion. Next to these systems to detect fraud, there are also systems that need to secure

that the received and given information is accurate and correct. These last quoted systems are also being used to be compliance approved; they ensure that everything is in line with the accounting and tax legislations.

The following two examples illustrate what might happen if these controls are not implemented.
The first example deals with the event of doubt about the correctness of the calculated numbers. As a result, it can be possible that the company is unable to publish the financial statements on time. This gives a very bad impression to the outside world which can result in investors asking the following question: 'If they even cannot meet the regulatory requirements, how are they capable of doing business?'. The next example is about lacking information. When a warehouse manager loads three trucks with products, ships them without recording this, it will of course cause problems. This is a situation that can happen when the controls are not working properly or when the people do not pay enough attention to them. One has to ask himself the question: 'Did we know that this risk existed?' If this is the case, why is this not being handled? If your answer to the first question is negative, one should wonder how it is possible that such a risk is not being noticed. In both situations the company damages its image, so one cannot say what is worse: not to know that this risk existed or to know that the risk exists and do nothing?

The company defines these risks, controlled by the internal audit, as 'unrewarded risks'. The reason for this description stems from the fact that there is only a limited, or even none, upside potential. If the risk does not occur, nothing would happen to reward the company. On the other hand, if the risk does occur, there will be downside effects.
Besides the 'unrewarded risks', the company defines 'rewarded risks'. These risks are treated by the Risk Management Process which is described in the subsequent section. These risks have the potential for positive effects next to negative effects. Meaning, when the risk is prevented from happening, there can be rewards attached to it. E.g. a competitive advantage by executing the strategy flawlessly.

A company needs to find the balance between internal control and efficiency. One can implement a sophisticated ERM process and a perfect internal control system, but an organization has to assess in that case if it is still selling products and if it is making a profit. Doing business always comes down to being profitable. On the other hand, one can produce high volumes and use lean methods to optimize the production and sales and neglect the internal control. A company cannot keep on producing in this manner if it does not comply with regulation and other requirements. The question then remains how sustainable both situations are. Therefore a balanced combination of both concepts seems recommended.

Figure 14. Balance between Internal Control and Efficiency

2. Risk Management Process

2.1. Registration of the possible risks

First of all, it is important to note that in this company, as in the first, everyone has the responsibility to look for possible risks. Moreover, everyone is encouraged to report the problems they are experiencing, so no potential risks are being overlooked.

The listing of the risks starts first with the internal control system. In this system, the company has systems and procedures to prevent risks from occurring. When this fails or when the internal control notices issues, this is being communicated to the responsible manager of the project or department, depending on the location of the risks.

Secondly, the issues are mostly being noticed via interviews or brainstorming sessions with interdepartmental groups. The latter ones are important to execute on a consistent basis, because not everyone assesses a risk with the same importance as anyone else. It is also crucial to determine the top 20 of most important risks (infra 'The Risk Assessment'), which are listed in these discussions.

All the problems and risks noticed by either the internal control or by the interviews or brainstorming sessions, are being registered and classified in the suitable group, as is explained in the next step.

2.2. Enterprise Risk management Structure

The second company applied a rather informal ERM structure, by the use of classifying risks. They allocate risks to four predefined groups. Those four groups are called the 'internal risks' and are the following: business risks, financial risks, operational risks and corporate risks.

Under business risks, the company understands the more broadly defined organizational and people risks. People risks are the risks of involuntary personnel leave, employees going on a strike, etc. The title of financial risks for the second group, speaks for itself. The credit risks and market risks are put in this category. Operational risks deal with the functioning of the company, so the technology that is present in the company must be safeguarded, the same with the machinery, but also legal risks are

classified in this group. The final internal risk group is represented by the corporate risks. Shareholder and reputational risks are the main topics covering this group.

Apart from the internal risks, they identified another group called 'external risks'. More specifically, these risks are country specific risks. When a company decides to invest in a new plant in a foreign country, it is important to look out for some major risks that may be typical for the area abroad. E.g. instable political situation, the possibility of an earthquake or a flood risk. In our literature review we also saw the example of an earthquake as a high-impact risk with low probability. There it was indicated that the most common technique to identify this risk, was the scenario analysis. Implicitly we can classify what this company does, under the name of this technique.

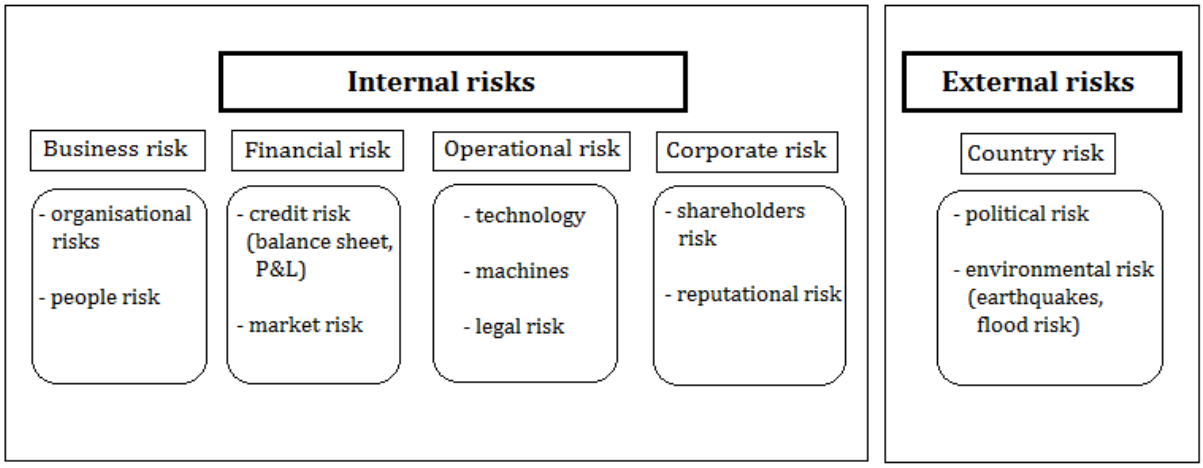


Figure 15. ERM structure

2.3. The Risk Assessment

After the classification of the risks is completed, the organization makes a top 20 of the most important risks. They do this by assessing the probability of a risk occurring and by looking at the impact. By the latter element, the company assesses 'If it would happen, what will it cost'.

The assessment is made clear to the rest of the organization by using heat maps. They also make use of an ERM roadmap which can be found in 'Appendix 6', where the first step is to set the objective, what the company wants to achieve. Step 2 identifies the event and determines the risk interaction, then the risks are assessed based on the impact and probability, as can be shown by a heat map. Risks that are likely and have a high impact are then prioritized, treated and monitored in the next steps.

Despite the use of these rather formal tools, the company claims they do not use any quantifiable methods to give a risk the status of 'top 20 – risk'. However, when we compare the use of the top 20, with our literature review, we can classify this under the risk rankings. The company says that it is not using specific techniques, but what they do in the risk assessment, is comparable.

Once the top 20 is chosen, these risks are the only ones the company is going to treat in the next step.

2.4. The Risk Treatment

For the risks that get to this point, the company first thinks of a possible insurance and secondly, if they can afford it. The latter question can be weakened a bit, because they look at the balance between risk premium and cost of risk happening and not per se at the absolute cost.

The second company deals with risks by entering in an insurance contract. In this way, the risk is being transferred. We will provide the reader with some examples of insurances the company has.

There can be a risk concerning the product, e.g. when there is a product defect, the company will need to issue a product recall, so a product liability occurs. The probability of these defects occurring is unknown so the company gets an insurance to cover this.
Concerning customers a credit risk exists. One only can be sure of a sales contract when the money is transferred on his bank account. For this specific risk, they take a credit insurance.
Also for transport a risk can occur. E.g. when you transport a product, there is always a possibility that the truck has an accident and your goods get damaged and get worthless. Solution for this is a transport insurance.

3. Responsibilities

Structurally speaking, the whole company is involved in managing risk. Every employee is concerned with the identification of risks and reports his experiences to the department manager. This happens based on interviews where all remarks and possible risks are discussed. As mentioned before this is an ongoing and repetitive process because certain risks may disappear and some new ones may make their entrance.

The Board of Directors defines the risk appetite of the enterprise and gives direction to the Chief Executive Officer who is the ‘owner’ of the risk management process and deploys the ideas to the managers. The CEO is also responsible for defining the structure and process of ERM. The Board of Directors and the Audit Committee request to implement an ERM structure to give the enterprise the possibility to manage risk on an explicit basis. When the managers have determined the top 20 risks for their company, they report the results to the Board of Directors, which is in its turn responsible for the monitoring of the management. This ERM structure is a good example of both the top-down reporting and the bottom-up approach. The figure below gives a visual representation of these approaches.

Figure 16. Responsibility structure

3.1. Objective

The major objective is that the risk management idea needs to be embedded in the corporate culture. People must be challenged to focus their attention towards the possible threats that their department may come across. It is however conceivable that despite of the efforts to identify these threats, some risks can be overlooked by the own department. The company tries to resolve this problem by working with cross-functional teams which should give different insights linked to the participating employees' specialism. In a cross-functional team it is common to combine a department with support divisions, like finance or human resources.

When a new project is under development, the people who created the idea should verify the likelihood that the project will succeed. This is done by a SWOT-analysis where the strengths are being assessed against the weaknesses and the opportunities against the threats. One criticism on using the SWOT-analysis is that it should be done thoroughly. This is not always guaranteed because employees assess their own project and are convinced that their idea will be successful. The company then needs to be sure that its people are critically enough to question their own project and map the risks that it brings along.

3.2. COSO components

The company based their internal control system and ERM structure on two papers that were published by the Committee of Sponsoring Organizations of the Treadway Commission. Since the enterprise is stock market listed they need to release the main features of their risk management process in the annual report. To get a structured overview, they used the five components model of COSO, below one can find how this is explained in the section of their annual report.

The Control Environment consist of three levels that carry out the ERM process. Within every entity, there is an accounting team who is responsible to compute the financial information. This information is then evaluated by controllers, each within the scope of their responsibility. At last, there is a general control department that reviews all the financial information and that composes the consolidated financial statements.

The Risk Assessment is also interpreted from a financial point of view. This means that there are measures to ensure that the financial reporting is done reliably and on time. They try to realize this by good communication and coordination between the different levels, by following guidelines and a strict follow-up system.

The Control Activities consist of the procedures and rules which are already described under 'Internal Control'. There is also close attention to the segregation of duties in important processes. Further we have the Information and Communication section which is seen as very crucial in the company. The process of the responsibilities, explained under 'Responsibilities', is a good example of the top-down and bottom-up communication and reporting. Monitoring is also mainly focused on changes in the application of financial rules.

They basically implemented this framework because of the regulatory requirement to mention their risk management attention in the financial statements. However the fundamental belief of the company concerns the sustainability of the risk management process, so they think COSO is rather theoretic. This can be a reason why it is mainly applied to the financial information. They tried to implement the theory in a rather pragmatic way and did not create a lot of formal rules and frameworks.

4. Investors and Compliance

The driving force for the implementation of a risk management process in this company is mainly prompted by the investors and the compliance with regulation. There was also an influence of not falling behind on the competition and being alert and up to date with the economic transitions. Investors have set some criteria for themselves to evaluate the company on being reliable or not, in the end they also take a risk. As mentioned before, they are compliant with the law of April 6, 2011, which requires that they mention how they practice risk management in the notes of the annual report.

In comparison with the previous company, they are not SOX-approved. However, this is not necessary since they do not have American investors who require this approval. They see a big advantage to the fact that they do not need to implement the SOX requirements, since this gives

more freedom in deciding how to do risk management. You have the opportunity to use your common sense and do not need to do tests that become an automatism in the long run. A disadvantage to not being obliged to comply with SOX, is the fact that you need to start from scratch, you need to take care of the education yourself.

5. The role of Consultants

A final topic deals with the role of consultants in the area of risk management. These consultants are people or organizations who present a new method of doing risk management to the company. E.g. they can make companies aware of the new ISO standard (ISO 31000). The consultant can also advice the company about which ERM program would be suitable for the company. But, mainly, consultants want to make companies aware of the 'need' to do risk management. Companies are not obliged to follow the advice of the consultant.

The company does not believe that consultants have a role that matters. The reason for this is that the consultant does not know the organization or market environment well enough to give advice about how to manage for risks. As a result, the company tries to do everything internally, without any external party interfering. Because of this, there are a lot of resources needed in order to accomplish good risk management. 'It is about using the means one has, in a structured way and without blowing it out of proportions'.
A positive effect from this can be found in the fact that the company always needs to look at the long term. The personnel asks continuously questions like 'What are you going to do with the standard' or 'how to keep it sustainable'.

On the other hand, the company does believe that consultants can play a role of meaning in an organization. Consultants bring all the information and procedures and rules together in an overview. As mentioned in the beginning, there should not be any surprises when putting everything together; one should know its organization or department.
The positive effect of this overview, is that it makes it easier to communicate risk management to the Board of Directors. This communication is essential because of the knowledge the Board has. The Board of Directors has experience in other countries, so they are able to make comparisons. Resulting from these comparisons, they can make suggestions for improvement.

Comparison Case study 1 and 2

When describing our two visited companies, we have noticed some differences, which are worth clarifying in this section.

First of all, their application of the Enterprise Risk Management program. In the first company this was very extended and well documented whereas in the second company, the idea of the ERM program was conceived more casual. An example of this is the Risk Assessment step in both companies. The first company uses quantitative methods to assess whether they are going to treat the risks, if they decide not to do this, they have an official 'Risk Acceptance form'. The second organization uses qualitative judgments and by consensus only treats the top 20 risks, disregarding the other possible risks. Nevertheless, we saw that both companies use an ERM program more or less like we found in our Literature Review.

Another big difference we noticed when we conducted our interviews, was about the use of COSO and ISO standards. More concrete, the amount of endorsement of those rather theoretic standards. In both companies these were being used, but only in the first company people said explicitly that they implemented those standards. In that company, our interviewees were very fond of these standards. In contrast, the second company was rather opposed to applying those standards. That company wants to do everything internal by developing company specific procedures and rules etc. However, in doing so, they lean upon the COSO framework more than they say. We can conclude that both companies use the COSO framework, the one with more conviction than the other.

Another comparison can be made in the area of responsibilities. In our second interviewed company, everybody in the organization has the responsibility to be aware of risks and report them when noticed. In this manner, the goal of risk management is to be embedded in the company culture. When we contrast this with our findings from our first company, we notice that responsible persons are appointed in every department. However, when there are problems, all employees need to report them, so possible risks can be noticed. When we look at the risk management process in that perspective, both companies are equal.

A last notable resemblance can be found in terms of 'risk education'. In both companies the personnel is educated so they can manage risks in the best possible way. The only minor difference remains with respect to whom these sessions are held for. In the first company, the responsible person for this education, gives presentations to the appointed responsible persons of the departments about how to do risk management. But, in the second company, mandatory sessions are organized for all new employees concerning internal control.

Questionnaire

In this part we will present our findings from our enquiry, which can be found in Appendix 7.

The questions are based on the treated topics in our literature study. To get an idea on the query formulation, we based our questions on the structure of the Accenture report (Accenture, 2011) and on an article from The Economist, Fall Guys (Fall guys - Risk Management in the Frontline, 2010). Some of the questions asked in these questionnaires return in our enquiry, this in order to get an idea on the evolution of the subject. We tested our questionnaire in two organizations and also Belrim was provided with a copy of the questions, which are closed multiple choice. After this pretest we adjusted some wordings and sequences of the questions before putting the survey online.

In order to get the respondents we needed, we cooperated with the Belrim association. Belrim stands for *Belgian Risk Management Association*. The goals of Belrim are twofold in that sense that they make a distinction between their national and their international objectives.
Nationally: They want to "*allow risk and insurance managers to compare their experiences and to discuss their problems*" and "*act as a spokesperson with regard to the authorities, the administration,[…]*".
Internationally: "*BELRIM is a member of the European Federation of Risk Management (FERMA), a platform dedicated to the exchange of information among the different national associations of more than 15 European countries.*" And "*BELRIM is a member of the International Federation of Risk and Insurance Managers Associations (IFRIMA).*" (Belrim, 2012).

This made Belrim our perfect partner. After eliminating for financial companies, we contacted 103 organizations that are associated with Belrim. Our goal is to investigate companies in Belgium that are already dealing with risk management so we can have an idea of the current state of affairs. Since we cannot know all Belgian companies that are already dealing with risk management, which is our population, we must use a known sample of companies that are already managing risk. We consider the 103 contacted companies as our sampling frame, which is defined as '*the list of all members of the population under investigation'.* (De Pelsmacker & Van Kenhove, 2010) Because these 103 companies have all '*a known chance, which is not equal to zero, to be selected*' (De Pelsmacker & Van Kenhove, 2010), we are using a probabilistic sampling procedure. Every company had the chance to participate.

Two weeks after we sent out the emails to complete our enquiry, we got 28 responses. Then a reminder with a time limit was released and we got to our final number of 39 responses. This equals to a response rate of 38 per cent.

1. Findings

In this section we will clarify our findings from the conducted survey on risk management in non-financial companies. We tried to reach as many companies as possible from diverse sectors to investigate if there was a distinction between them concerning the implementation of risk management. Though we have a reasonable sampling, we advise to be cautious in making general statements.

1.1. Company profile

A finding that contributes to the credibility of our study is that almost half of our respondents are Risk Officers which indicates that our questionnaire is being filled out by people who have knowledge of risk management. A lot of respondents also marked the "other" option. When we take a closer look at this choice, we see that 22 per cent are people that are related to the risk management function. A cautious conclusion from this is that half of the companies that responded to our questionnaire have already a specific risk function in its place. Another fifth of the companies do not have a specific function, but have already created functions where a large part of the focus is on risk management. From our interview with the first company, we know that even if there is no distinct link to risk management in the name of the function, these people may be involved in it. So we can conclude that our questionnaire has been handled by the right people.

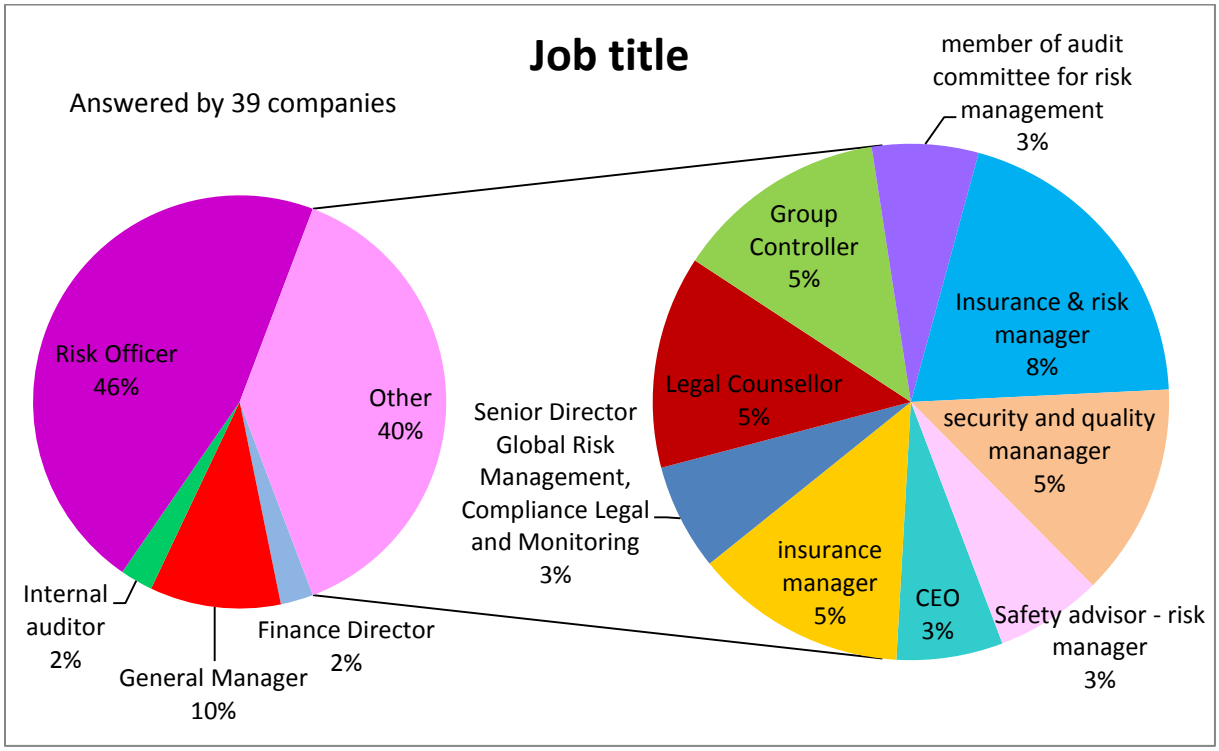


Figure 17. Job title

The most prominent sectors in our research were Logistics, High Tech Industry, Healthcare and the Public and Social Profit sector, they count for 39 per cent of our sample size. We got responses of at least one company in 21 different industries. The pie chart shows the detailed distribution of the sample by sector. In our enquiry there were 10 predefined categories, those companies that did not register in one of these, were assigned to the "others" group and could indicate in which other industry they are active.

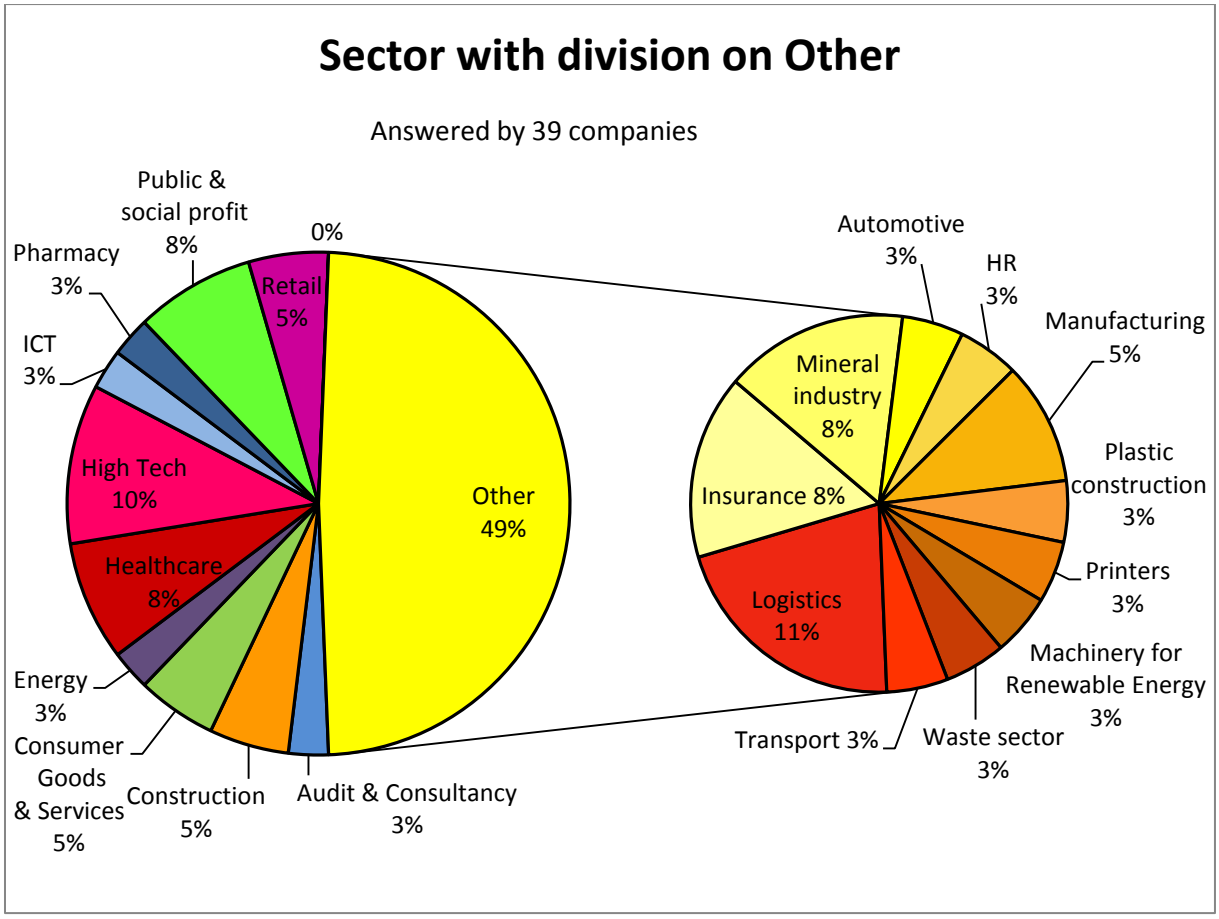


Figure 18. Sector with division on Other

Most of the companies that completed our questionnaire have a headcount of over 1.000 employees. On the other hand, all the interviewed companies have a headcount of no less than 100 employees. Therefore they can be all classified as large enterprises according to the size criteria of the National Bank of Belgium. Because of their classification as large enterprise, they are obliged to publish the full format of the financial statements.

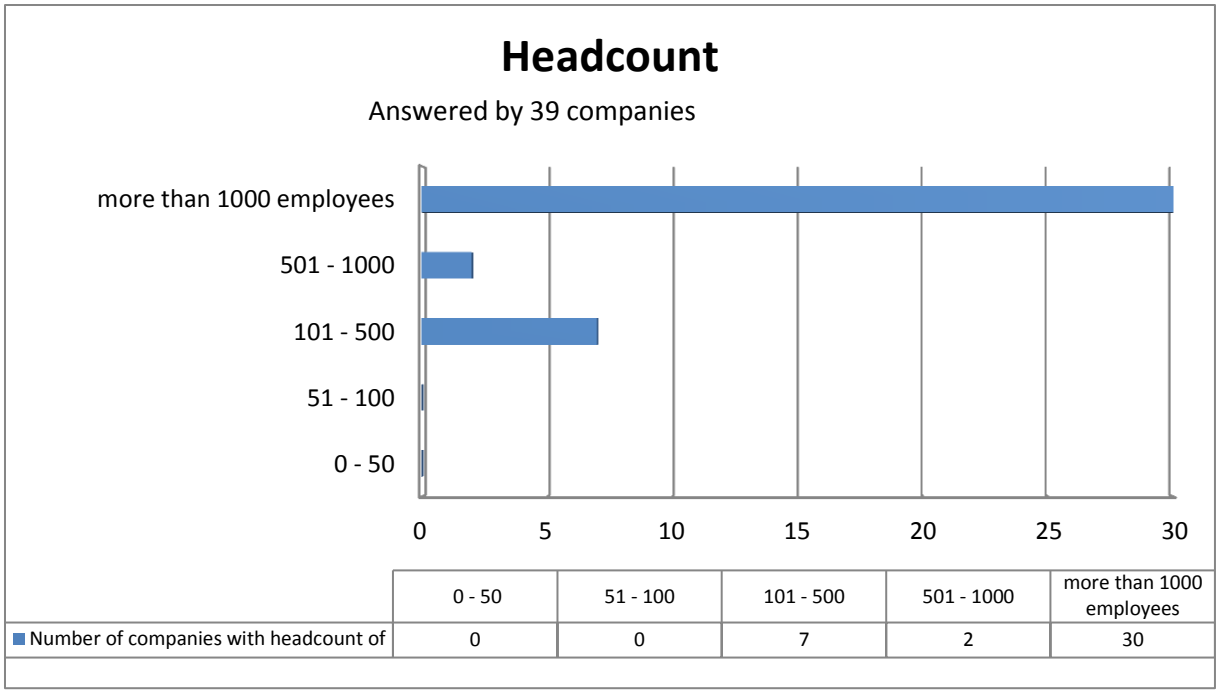


Figure 19. Headcount

The participating companies reflect their size in their turnover. The two largest groups that draw attention are the ones with a turnover of less than € 150 million and another one between € 150 and € 300 million. But as you can see on the graph, our enquiry has also been completed by much larger firms. One observation is that the company size can have an impact on the implementation of risk management and on the available resources to address the risks that may occur. From our research we can derive that most of the companies that are not using a risk management program, can be classified in the two lowest turnover categories. So size matters in implementation of risk management.

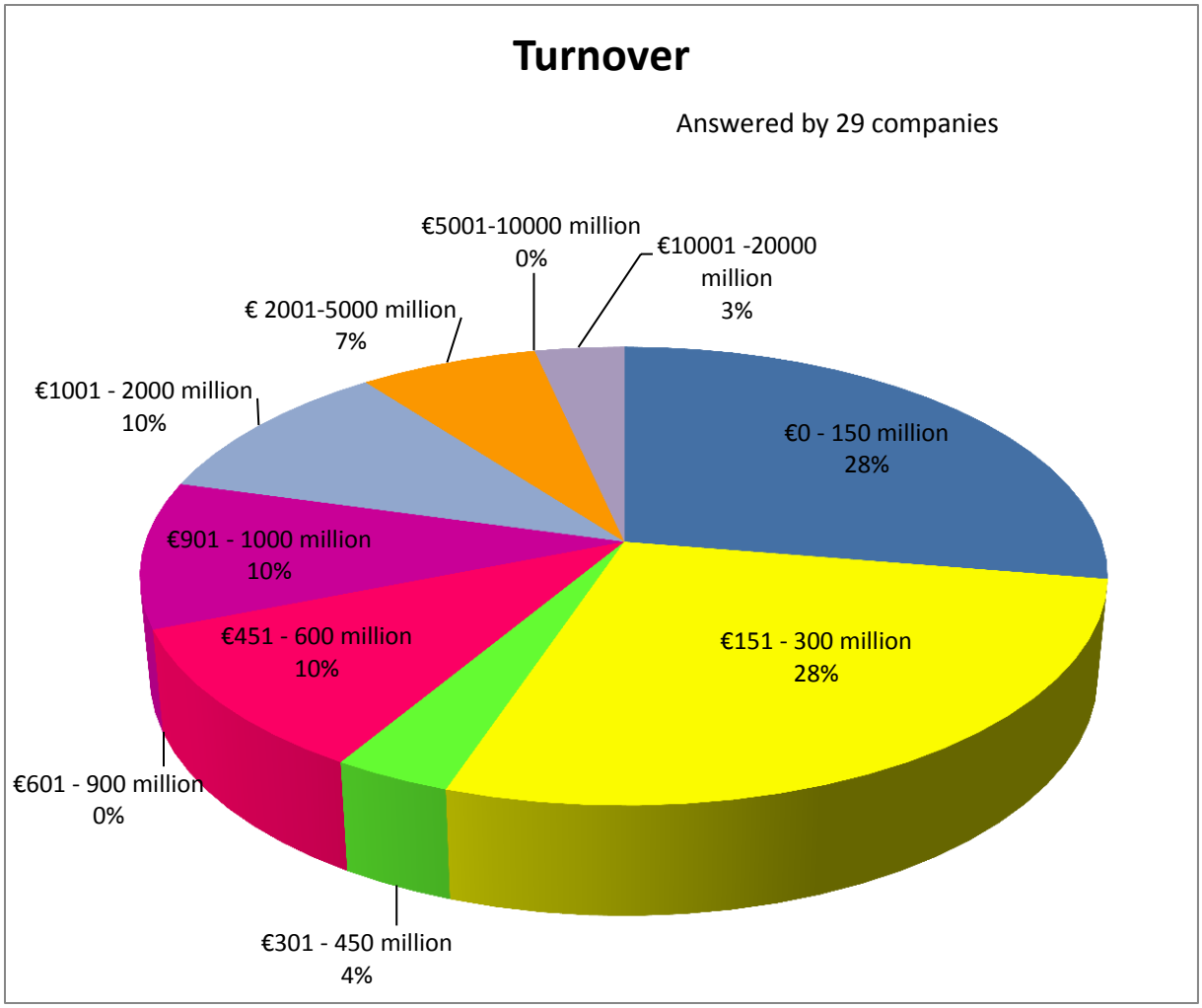


Figure 20. Turnover

1.2. Company awareness

Our first research topic was about the knowledge of the companies of the law of April 6, 2011. We have enlightened this topic in our literature review in section 8.1.4.. We stated that certain rules of the new obligation for listed companies, to mention their main features in the annual report, were not being respected. These provisions related mainly to risk management. In order to know why this was not being respected, we asked the companies if they knew there was a new law concerning risk management. Of the 37 companies that answered this question, only 10 organizations were unaware of this new law. This unawareness will result in the provisions being neglected.

We also wanted to know, when the company was aware of its obligations, what the impact was of mentioning their main features in their annual report. We wanted to know this because this new law should have had some impact at risk management since the government would otherwise not have published this law. At first sight, there was mainly no impact, but in this answer were also included, the 10 organizations that did not know this law existed. Obviously, all 10 companies had indicated

that there was no impact of this new law in their company. Of the 27 companies that were aware of the provisions another 10 companies indicated that there had been no impact. An explanation for this can be found in the fact that of the 103 contacted firms, only 40 per cent are listed. Since the rule only applies to listed companies, it could be expected that a large part of our respondents encounter no impact of this law. This could also be an explanation for the 10 companies that did not know the new provisions. The 17 companies that indicated that they noticed an impact of this law mainly stated that this impact resulted in more attention towards risk management. Better monitoring of existing procedures and/or standards came in close second. Another large part even indicated that they applied new procedures and/or standards.

We can state that for the companies in our study, this new law has had a slightly more positive impact on risk management than no impact.

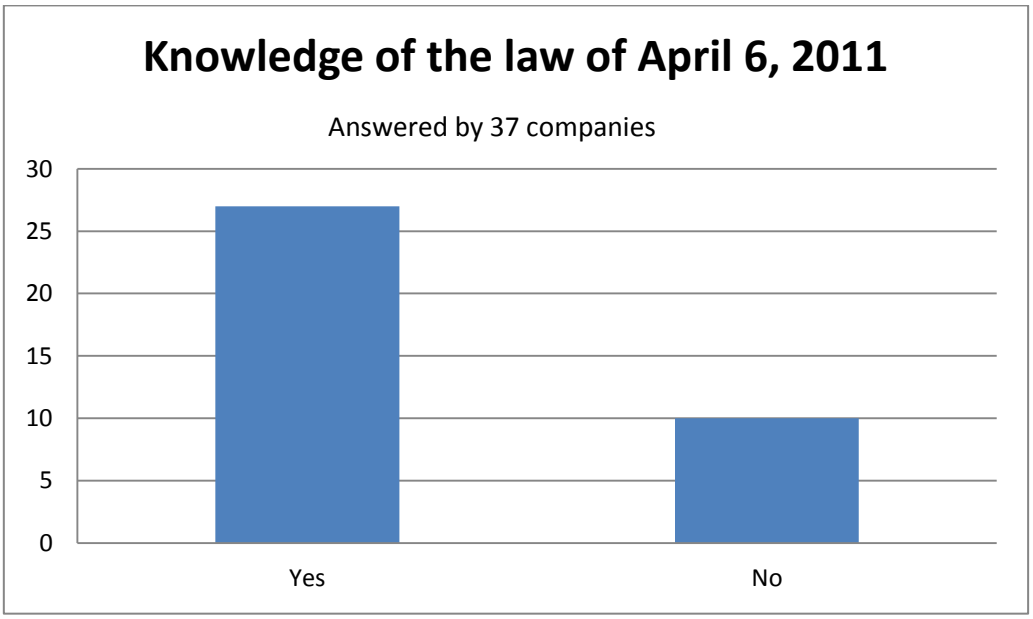


Figure 21. Knowledge of the law of April 6, 2011

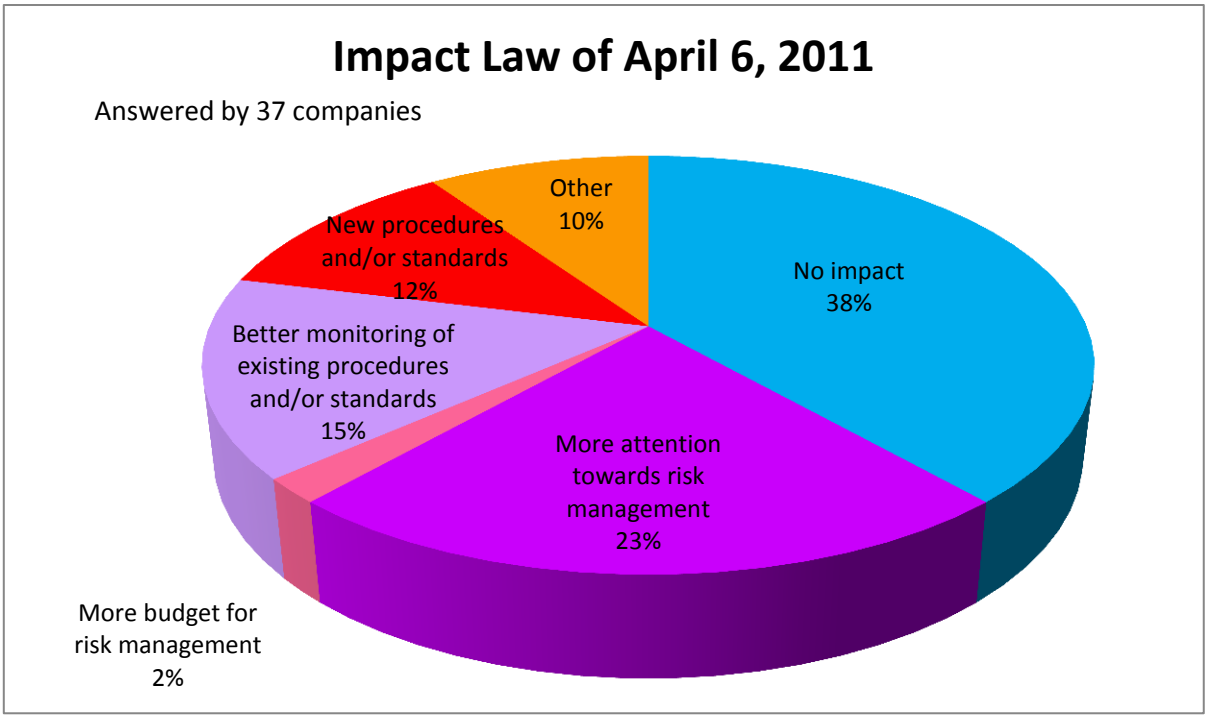


Figure 22. Impact Law of April 6, 2011

In the same section of our literature review, about the requirements of the new law of April 6, 2011, we also made an in-depth analysis of the guidelines that the Corporate Governance Committee has worked out to simplify the requirements. We have asked our respondents if they were aware of these guidelines to help them implement the law. Only 40 per cent of the companies knew these guidelines exist. 60 per cent of the companies that answered this question indicated that they were unfamiliar with these guidelines. Keeping this in mind, we should not be surprised that a stunning 70 per cent does not use these guidelines.

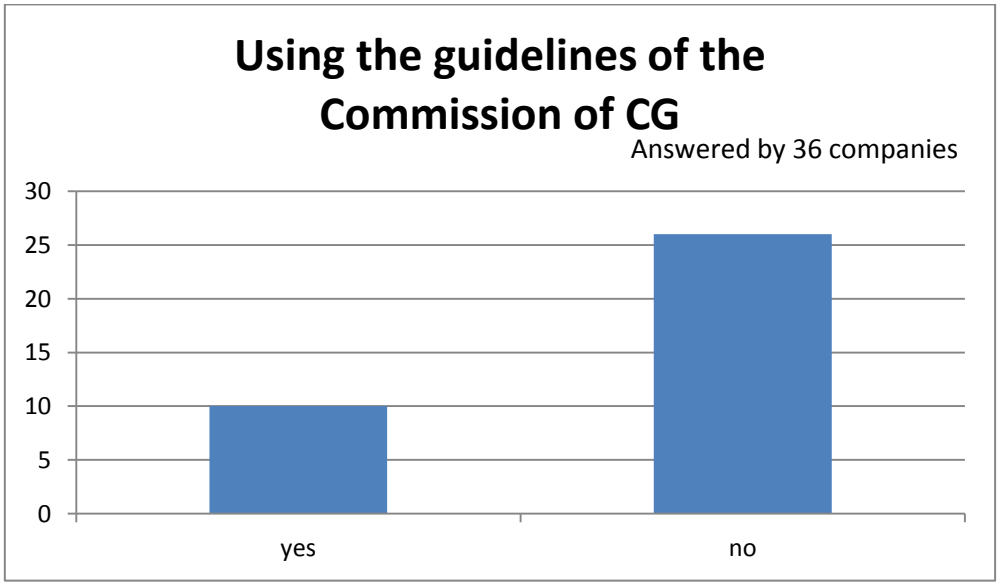
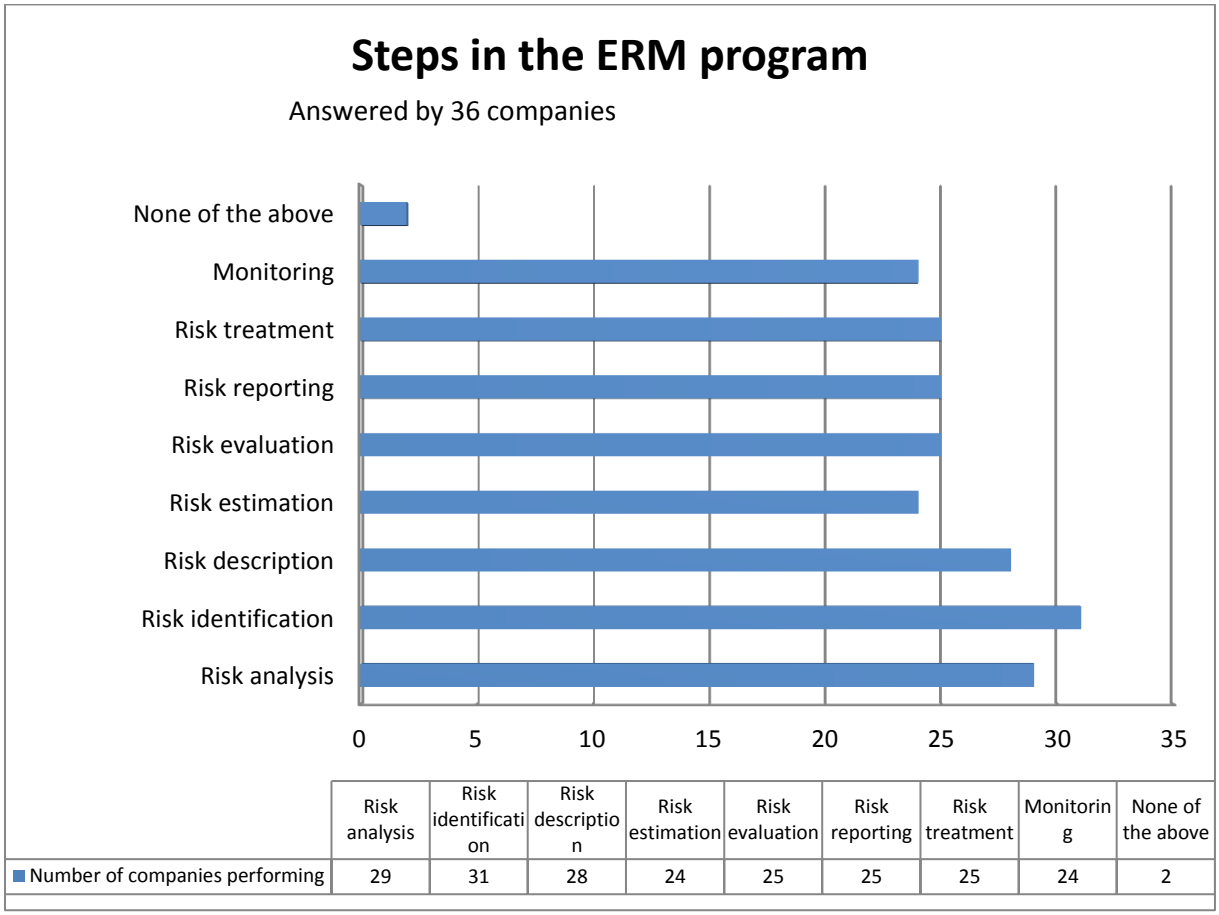


Figure 23. Using the guidelines of the Commission of CG

1.3. ERM program

When we take a look at the implementation of risk management programs, we notice that still 25 per cent of our sample does not have a risk management program at all. We need to discern this percentage a little more, because only 2 companies implemented not a single step of any ERM program. The others do implement risk identification, risk description and sometimes risk analysis in their company. The step that is mostly performed is the risk identification, which is however closely followed by risk analysis and risk description. Risk estimation and monitoring are the least applied steps, but this difference in implementation is almost negligible.



	Risk analysis	Risk identification	Risk description	Risk estimation	Risk evaluation	Risk reporting	Risk treatment	Monitoring	None of the above
Number of companies performing	29	31	28	24	25	25	25	24	2

Figure 24. Steps in the ERM program

1.4. Risk perception

Further we can say that the risks that are perceived as the most important for the sector, match more or less those of the individual company. Notwithstanding, there are some noticeable differences in the significance of the liquidity and technical risk. The liquidity risk is twice as large for the sector than it is for the individual company. Firms perceive their own risk of liquidity problems much smaller than that of the other companies in their industry. The opposite is being observed for the technical risk, this is 17 per cent for the individual company and merely 9 per cent for the sector.

The biggest risk is the operational risk, followed by the technical and reputational risk. Some companies made us aware of the fact that they see some other risks as more important. Mentioned are: the political risks, the fraud and IT risks and the risk of degradation of the internal demand.

Since our sample size is rather small, it was not so easy to derive the most important risks for every sector separately. Even though these results were computed via crosstabs and bar charts. The reader should be cautious concerning the interpretation of these results. We got *one* company from the Audit and Consultancy sector, the Energy sector, ICT and Pharmacy who answered our questionnaire. *Two* enterprises from Construction, Consumer and Service Goods and Retail sector. *Three* from Healthcare and Public and Social Profit sector, *four* companies from the High Tech industry and *nineteen* companies who are classified in the ”other” category.

The results will be described for the sectors that contain more than one observation, the accompanying graphs can be found in the Appendices (Appendix 8). For the Construction sector the most important risks of the two companies did not match. Market risk, operational risk, reputational risk, technical risk and weakening demand were mentioned as being the most significant. For the Consumer and Service Goods there were also no similar risks indicated by both companies. The mentioned risks are liquidity risk, operational risk, reputational risk and strategic risk. The two companies from the Retail sector however both indicated operational risk as one of the most important risks in their sector.

Research in the Healthcare sector showed us that two of the three interrogated companies indicated operational and strategic risks as the major risks in this sector. Also reputational risk and compliance have an influence, one company stated that political risks should be taken into account. In the Public and Social Profit sector it is the reputational risk that is of great importance. Another mentioned risk in this sector is fraud.

Three of the four respondents from the High Tech industry reported that they perceived the compliance risk and the strategic risk as the biggest risk factors in their industry. Further also the operational risk seems to have a moderate impact on the business activities.

Next we got the results of the biggest category in our sample, more concrete of the “others” group. This category consist of all sorts of industries, so the interpretation of this category is not as valuable. The market risk seems to have the most important influence but is closely followed by the operational risk, weakening demand and compliance risk.

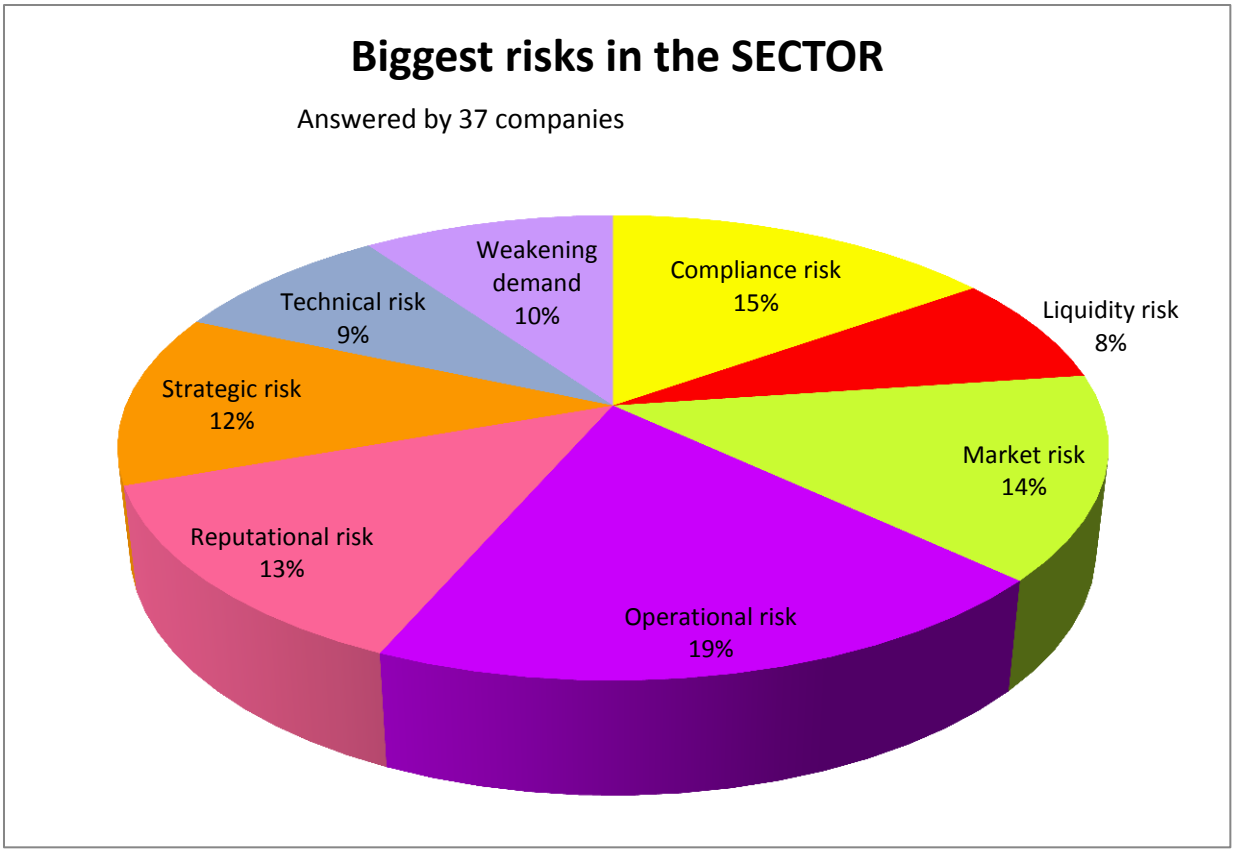


Figure 25. Biggest risks in the sector

Figure 26. Biggest risks in the company

1.5. *Risks currently being measured*

Now that the most important sector risks and company risks are revealed, we can examine which risks our surveyed companies are currently measuring. As seen before, the operational risk is considered as the most important one, this is also the risk that has mostly been measured, by precisely 72 per cent of the entities.

Next are the business risks, this is a wide category that grasps all sorts of obstacles that companies have to deal with. Some examples of this category are the declining sales volume, the higher input costs, the changing overall economic climate, the fierce competition, etc. This risk is being measured in 69 per cent of the cases. Further on we still have two risks that surpass the 50 per cent level of measurement: the legal risks and the credit risks. It is important to keep track of legal risks because they can have a direct influence on the business prospects of an entity. 59 per cent of the companies report to gauge this effect. The technical risk that was perceived as the second most important one is measured in 44 per cent of the companies and therefore belongs to the lower measured ones. The least gauged risk is that of the regulatory requirements. Only one company stated that they are measuring not one single risk.

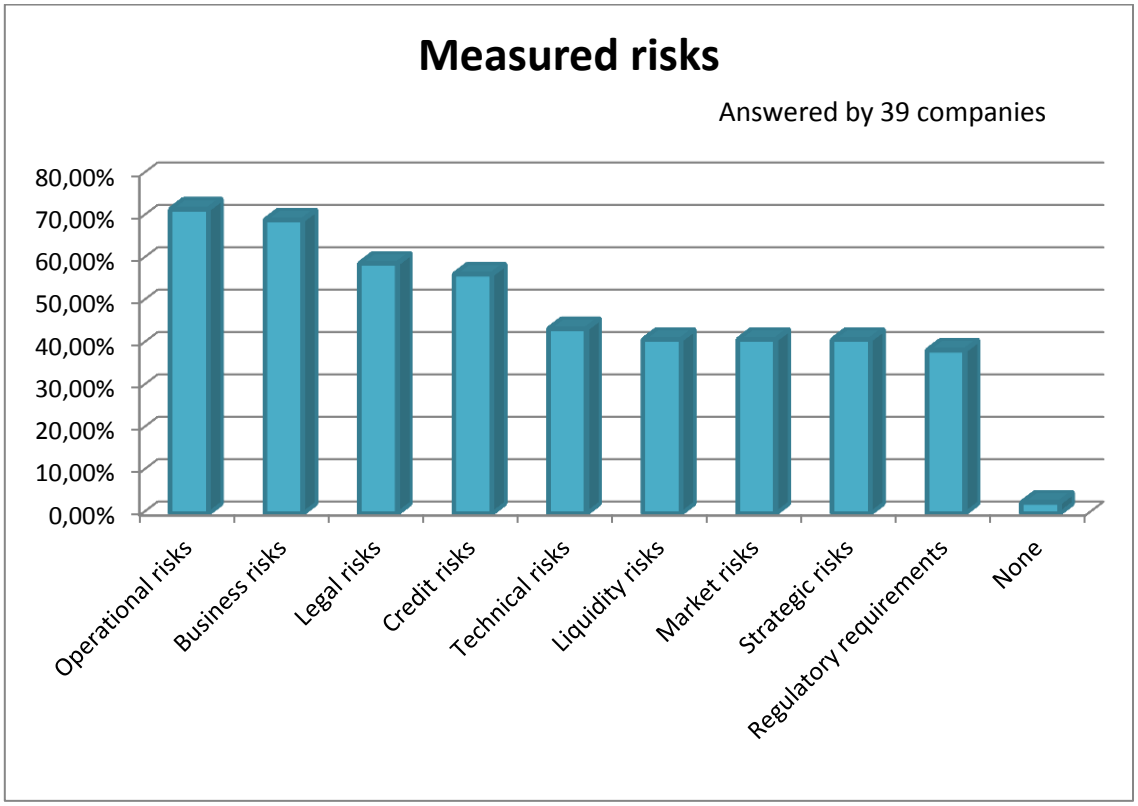


Figure 27. Measured risks

1.6. External factors and stakeholders

All these risks are being measured so that companies can manage them. Often is risk management triggered by external factors, so our next goal was to measure which stakeholders or externalities have a strong influence on the organization.

Generally speaking, customers are the most important stakeholders. With an outstanding 27 per cent they represent the most significant group. By generally speaking, we mean that we did not ask this as applied to risk management. The reason that customers are chosen by almost a third of the companies results from the fact that without customers, there would be no company. Management makes a close second with 23 per cent. The government, employees and investors all are around 10 per cent. Banks and insurers appear not to have a large perceived influence. Our attention was also drawn to the impact of the Board of Directors.

When we look at the external factors that have an influence specifically applied to risk management, we notice that legal requirements play a large role in 31 per cent of the cases. This in contrast with the 13 per cent the governance received as having a strong influence on their organization. It appears that the government has a bigger impact on risk management than it has on the entire organization. Moreover, compliance is also well represented within the risk management. This is with 28 per cent the second largest category.

Another remark that we can make, is that companies rate catastrophic events on the same high level as pressure from the market. Respectively 19 and 18 per cent, putting them at a third and fourth place. This is remarkable because when we ask about the more general influence of stakeholders, pressure from the market is judged as being the most important. Under pressure from the market we understand the influence of customers, insurers, investors and rating agencies. All being external from the organization with their own interests thus creating their own pressure on the company.

As other external factors, the companies pointed to strategy, the Board of Directors and just an increased risk awareness. We did not include these factors in the possible answers, since we do not consider these as being external.

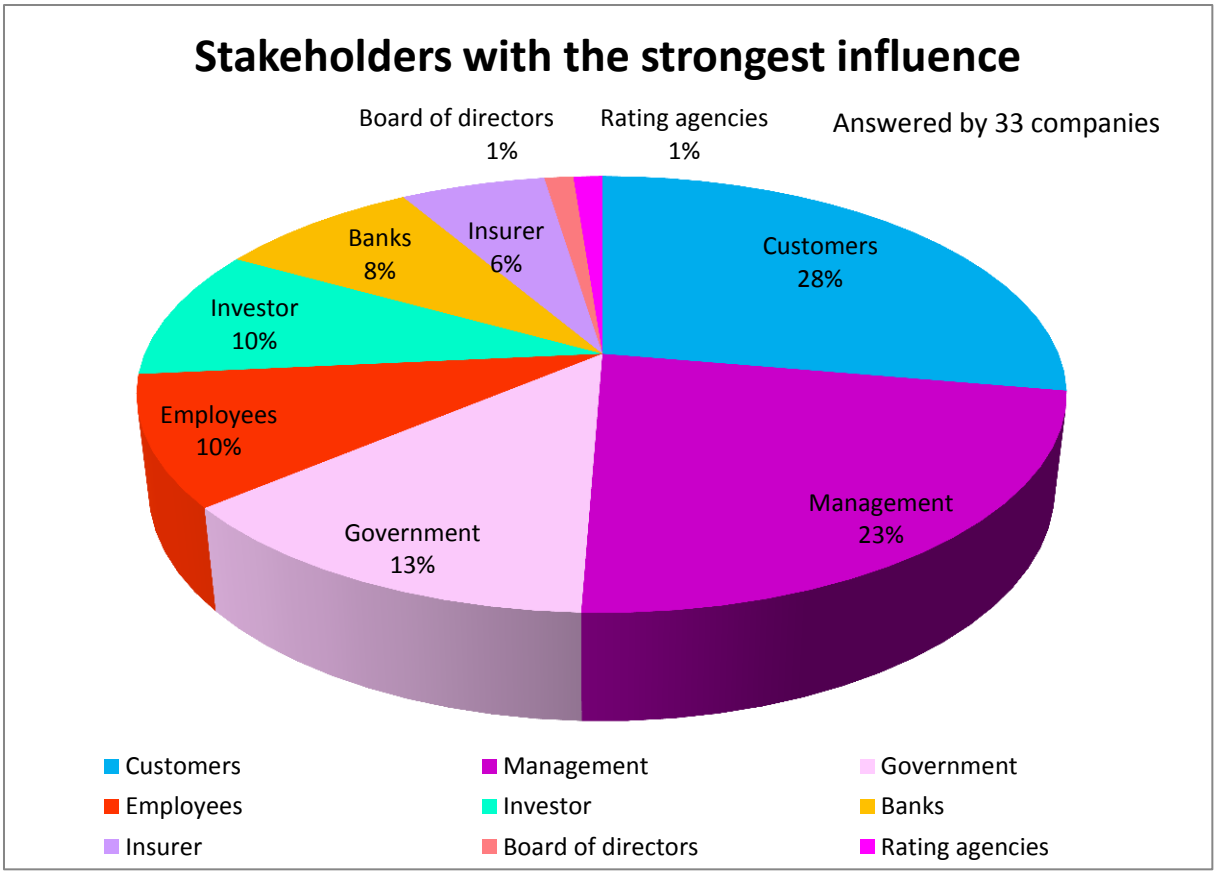


Figure 28. Stakeholders with the strongest influence

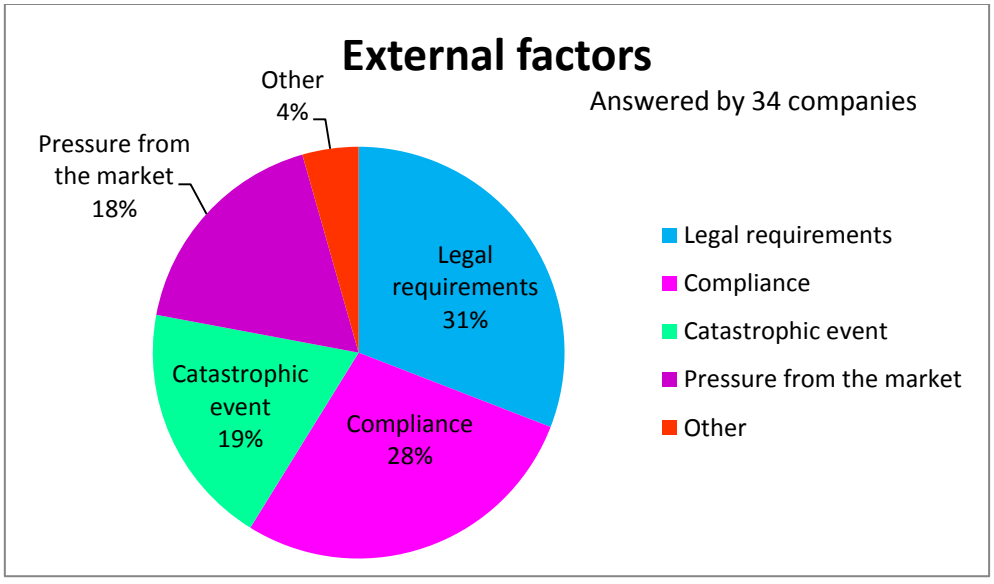


Figure 29. External factors

1.7. Who is responsible for risk management?

Now that we have established which risks are important, which are being measured, how companies perform risk management and what the main external trigger is for risk management; it is time to explore who is responsible to keep the risk management on the right track. With 26 per cent, the line management is chosen as being responsible for managing risk. However, they are closely followed by

the Chief Risk Officer who was elected by 25 per cent of the companies that answered this question. This intriguing result, of picking the line manager over the Chief Risk Officer, can perhaps be explained by our previous, cautious analysis on who answered this questionnaire. We stated that a fifth of the companies perhaps do not yet have a concrete risk function in their company. Hence, the responsibility falls on the shoulders of the people dealing with the risks on a day to day basis, which is the line management. Also a large number of the companies elected the finance department as being responsible.

Internal audit and internal control appear not to have a role of responsibility in the risk management in many organizations.

We can see that 16 per cent of the companies who selected the option "other", say that it are mainly the people at a more corporate level who are responsible. This is also a reason why we can conclude that in all the companies that filled out our enquiry, risk management is being taken very seriously. The risks are all being managed by managers at a higher level in the organization.

Another interesting conclusion that we can make about the person responsible for risk management is that of the 18 persons who said to be Risk Officers, 6 did not point to the Chief Risk Officer as the one being responsible for managing risk. Four of them indicated that the line management is responsible, one named the Managing Director and the last one pointed at the corporate level. All of this helps us to understand why only 25 per cent chose the Chief Risk officer; knowing that 46 per cent of the respondents is a Risk Officer. Nevertheless, this remains an interesting phenomenon.

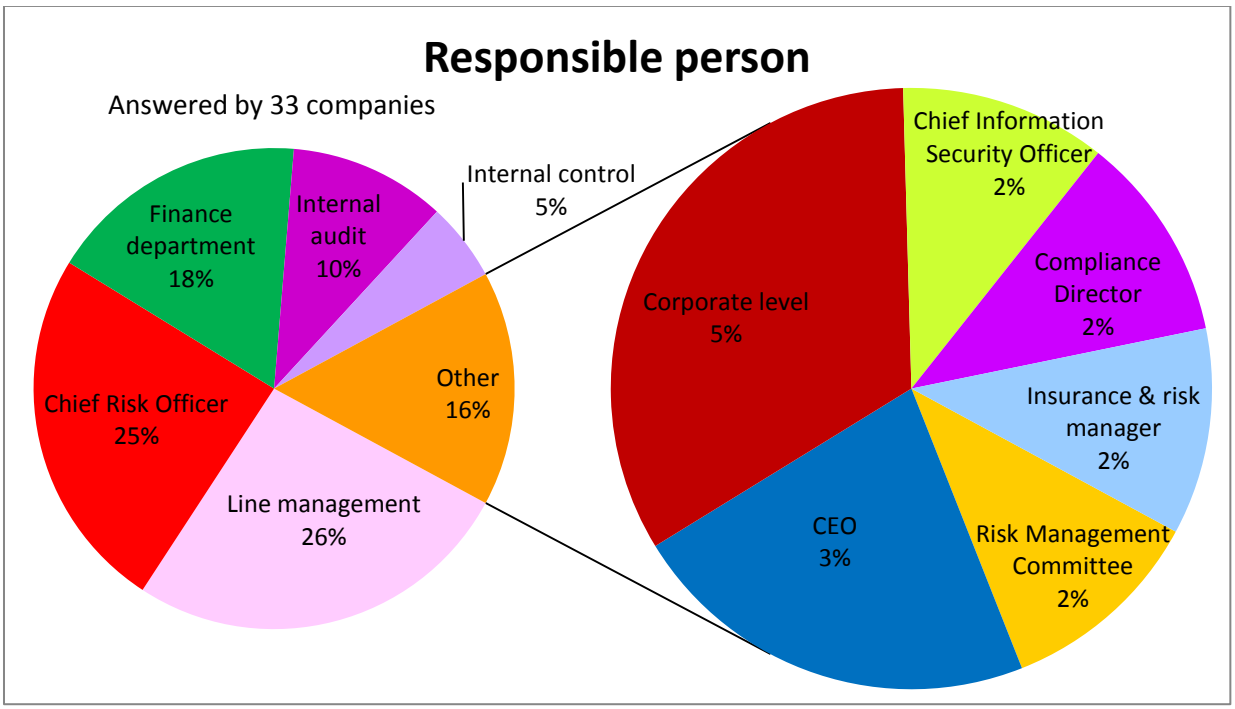


Figure 30. Responsible person

1.8. *Objective of Risk Management function*

When we asked the companies what they thought was the most important objective of the risk management function, the organizations answered that the risk management function should make it possible to take better managerial decisions and to implement a risk culture that is embedded in the strategy of the company. These two objectives are seen as prominent by respectively 37 per cent and 34 per cent of the companies. When only 25 per cent of the companies have a concrete risk management function with real responsibilities in risk management, we must approach this question from another angle. Our question should be, 'What do you want the most important objective of the risk management function to be?'. Next to the two, already mentioned, most prominent objectives, also the measurement and monitoring of the most important risks are seen as a competence of the risk management function. Ensuring compliance with regulation is not a big concern for the responsible for risk management as no company indicated this as an important objective. Other indicated points of interest are the alignment of the objectives of the different affiliates and dealing with the uncertainty of realizing such objectives. This also relates to the effective implementation of the company strategy with a view on long-term survival. The risk management function should also assist the entity in avoiding a major disaster or even bankruptcy to happen.

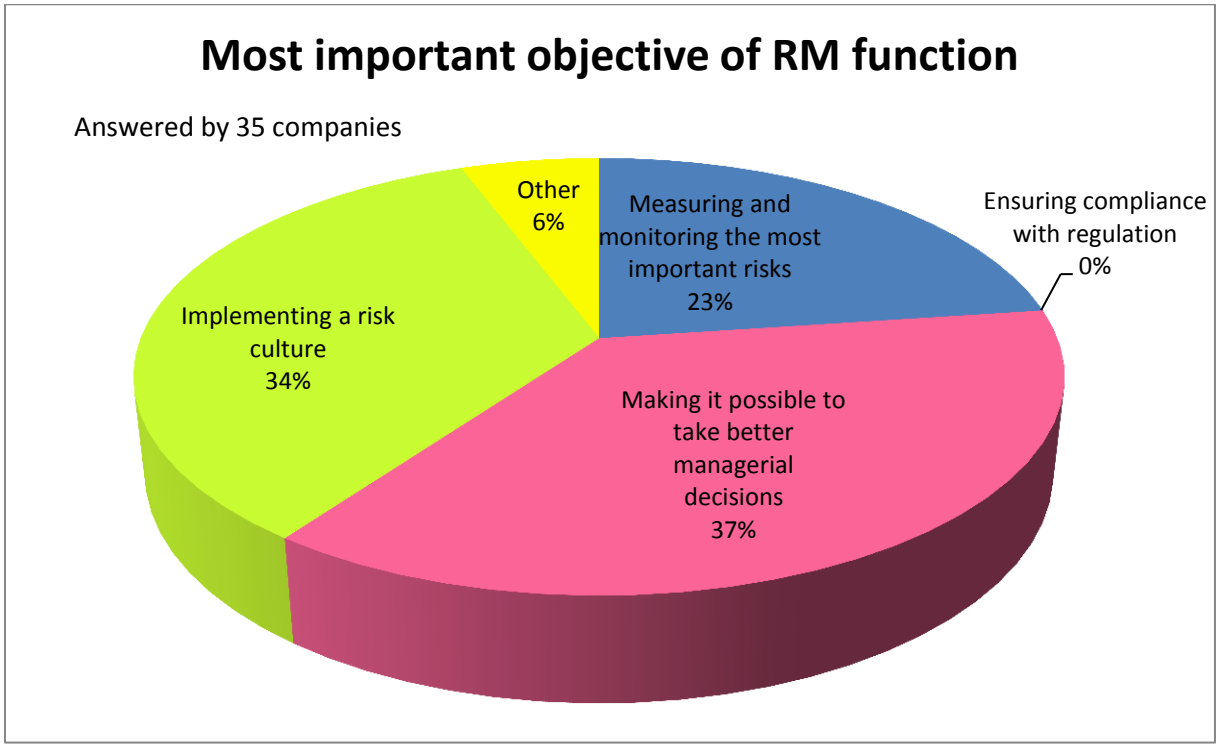


Figure 31. Most important objective of RM function

1.9. *Contribution of Risk Management to the company*

Moving on with this topic, we can expand our research to the area in which companies expect risk management to make the most meaningful contribution. Most results are in the area of addressing

stakeholders concerns and in compliance with regulatory requirements. Although this last one is not perceived as an important objective of the risk management function, 27 per cent of the companies expect to notice the most meaningful contribution in this area. Some entities stated other objectives as more relevant to observe the effect of risk management. Companies foresee risk management to support the design and the implementation of the strategy, to help improve decision making, to increase the risk awareness, to manage uncertainty on an explicit basis and to anticipate obstacles that obstruct the fulfillment of the company's objectives.

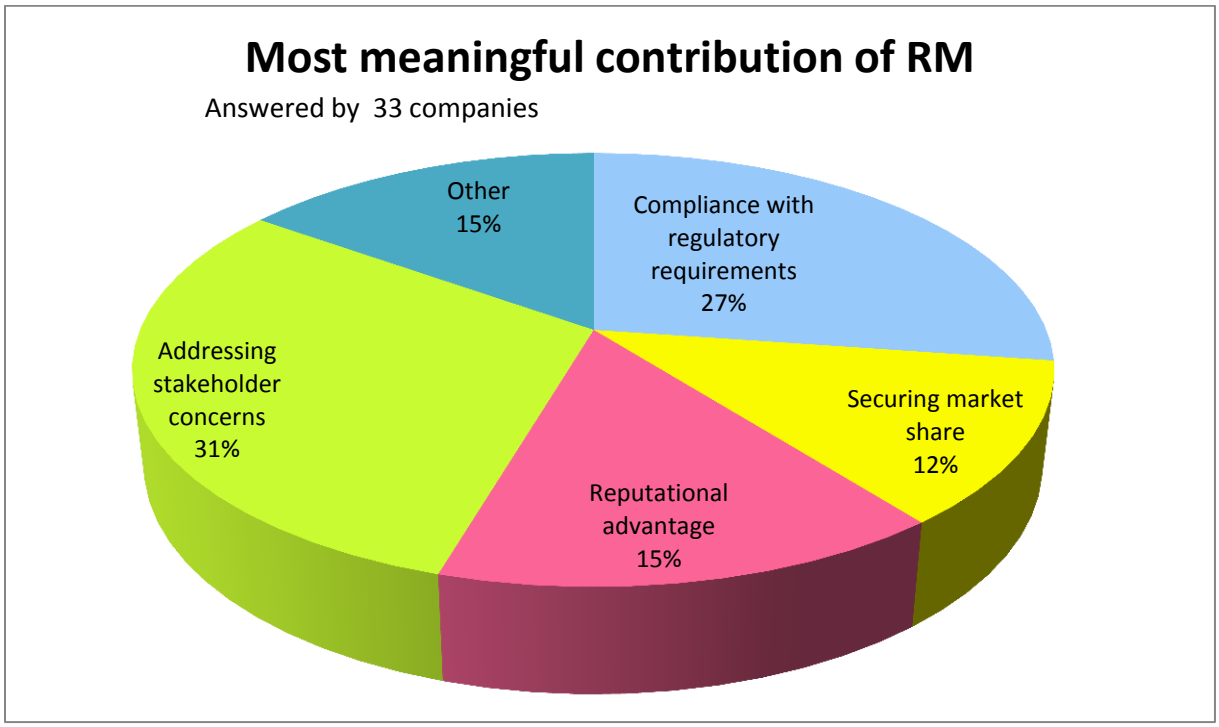


Figure 32. Most meaningful contribution of RM

1.10. Effectiveness

It was important to us to get an idea of how companies rate their own effectiveness on some concepts related to risk management. We examined this on a five-point scale where they could choose between the options: "highly effective", "more or less effective", "not specified", "not so effective" and "not effective".

First of all the link between risk management and corporate strategy was examined. From previous questions we already know that the implementation of risk management in the corporate strategy is seen as an important task of the risk management function. Risk management is also expected to support the implementation and the design of the strategy. From the literature study it is clear that risk management is only highly effective when it is fully implemented in the overall company strategy. 42 per cent of the enterprises stated that risk management and corporate strategy are

more or less effectively linked in their organization. 18 per cent even declared that their company was highly effective on this statement. This seems a rather remarkable result since 25 per cent of the companies said that the most significant barrier for effective risk management is the difficulty to implement this concept in the corporate culture (see 1.11. Barriers). Therefore we need to become aware of *the difference between a corporate strategy and corporate culture*. The culture deals with the values and behaviour of people in an entity, these are highly embedded and not easy to change. Strategy deals with the achievement of the company objectives but needs to be adjusted to recent changes in the economic environment, like the implementation of risk management. So for a strategy to be effectively executed, a suitable corporate culture is essential. Presumably this is the reason why 21 per cent of the companies rate their enterprise as not so effective on this statement: their personnel is not incorporating the concept as part of the company culture.

Figure 33. Linking risk management with corporate strategy

Moving on with this statement, we verified the effectiveness of the implementation of a risk culture. By risk culture we mean that all employees in the company are conscious of the risk exposures of their enterprise. There needs to be a common understanding on the influence of the risk culture on decision making and on the achievement of the overall objectives. 50 per cent rate their company as more or less effective on the implementation of a risk culture. In comparison with other questions concerning this topic we presume that companies are somewhat too optimistic in assessing this effectiveness because as said before, this implementation is seen as the most important barrier for risk management. Another 14 per cent rates their company as highly effective and just 18 per cent as not so effective.

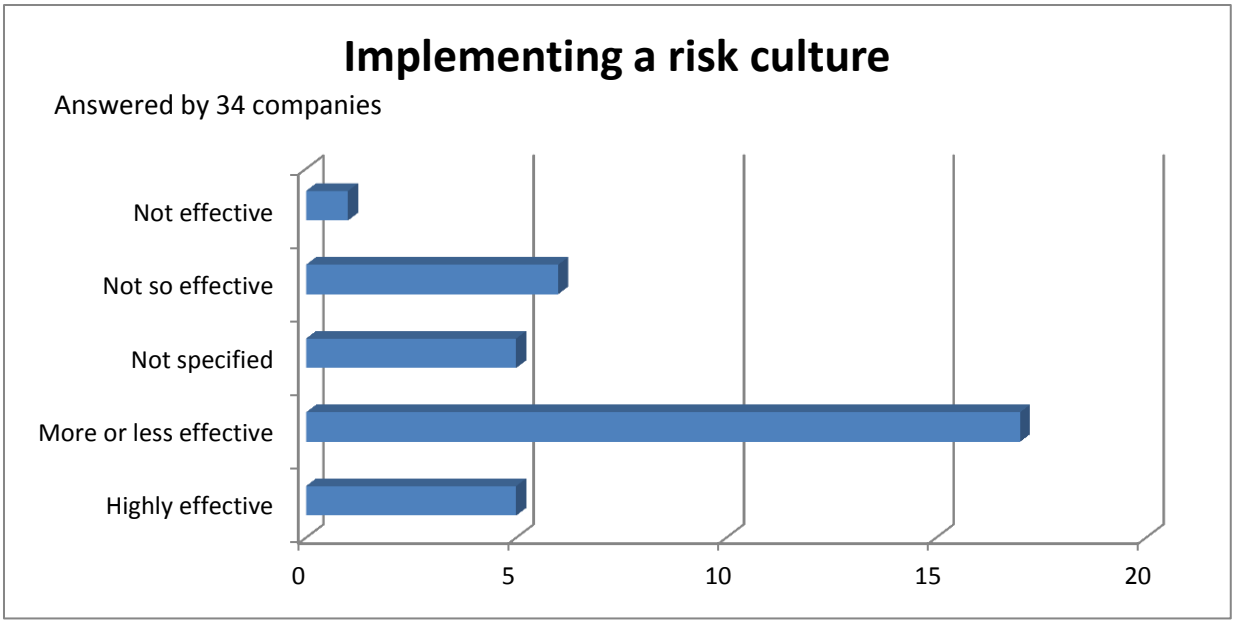


Figure 34. Implementing a risk culture

Next, the communication of risk information to investors had to be evaluated. It is curious that 27 per cent of the companies declared that this is not specified. Another 30 per cent state that their company is more or less effective in the communication of this information to their investors. When looking for an explanation for the high number of not specified answers, we checked the sector of these enterprises. It could be possible that this question is less relevant for e.g. enterprises in the Public and Social Profit sector. However, this did not contribute to an explanation of this figure, also the turnover could not lead to any decisive answer. Therefore we conclude that companies do possibly not dispose of this information or are not willing to give us an indication concerning this statement.

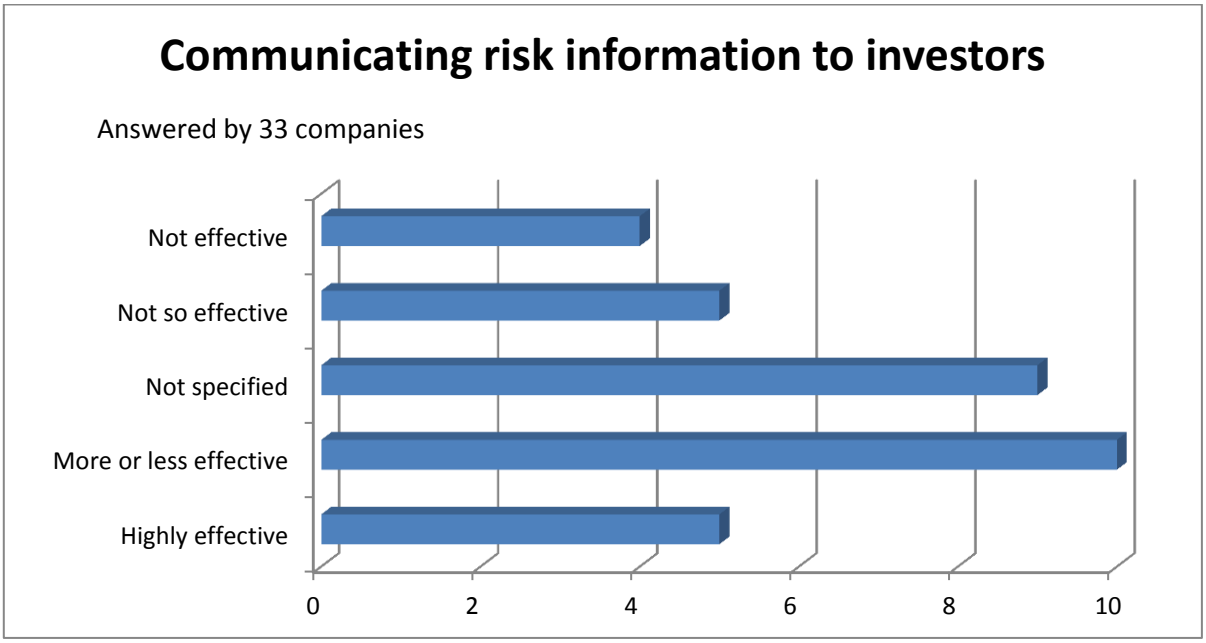


Figure 35. Communicating risk information to investors

Related to the previous notification, the effectiveness of the communication of risk management to the Board of Directors was assessed. Compared to the communication to investors, where 27 per cent said that the communication was not specified, only 9 per cent of the entities reported this in the case of communication to the Board of Directors. Most of the other companies found that their risk management information was reported more or less effective to the Board, more concrete, 41 per cent and even 38 per cent declared that this communication was highly effective. As mentioned in our literature study, the Board of Directors was recently assigned a role in the risk management of the organization. Their task is to guarantee a distinct description of the risk management policies, practices and performance. For this purpose a good communication is to the advantage of the company.

Figure 36. Communicating risk management information to the Board of Directors

Subsequently, two statements with reference to the regulatory compliance were enquired. The first one questioned the effectiveness of managing regulatory compliance. For the second statement we used a different undertone and asked the companies how effective they were in ensuring compliance with regulation. 33 per cent declared that their company managed regulatory compliance highly effective and another 39 per cent more or less effective. With the description of ensuring compliance with regulation even 52 per cent rated their company as more or less effective and 24 per cent as highly effective. Since these answers should give us more or less the same impression, we computed a crosstab to check the consistency of the answers. From this table it is clear that from the 33 per cent who answered “highly effective” on the statement of managing regulatory compliance, 18 per cent also answered “highly effective” on the other statement. Also for the other categories it is clear

that the answers for both statements more or less match. This was the result we expected to obtain by this different formulation.

Managing Compliance with regulation * Ensuring Compliance with regulation Crosstabulation

			Ensuring Compliance with regulation				
			Highly effective	More or less effective	Not specified	Not so effective	Total
Managing Compliance with regulation	Highly effective	Count	6	5	0	0	11
		% of Total	18,2%	15,2%	,0%	,0%	33,3%
	More or less effective	Count	2	10	1	0	13
		% of Total	6,1%	30,3%	3,0%	,0%	39,4%
	Not specified	Count	0	2	3	0	5
		% of Total	,0%	6,1%	9,1%	,0%	15,2%
	Not so effective	Count	0	0	1	2	3
		% of Total	,0%	,0%	3,0%	6,1%	9,1%
	Not effective	Count	0	0	0	1	1
		% of Total	,0%	,0%	,0%	3,0%	3,0%
Total		Count	8	17	5	3	33
		% of Total	24,2%	51,5%	15,2%	9,1%	100,0%

Figure 37. Crosstab regulatory compliance

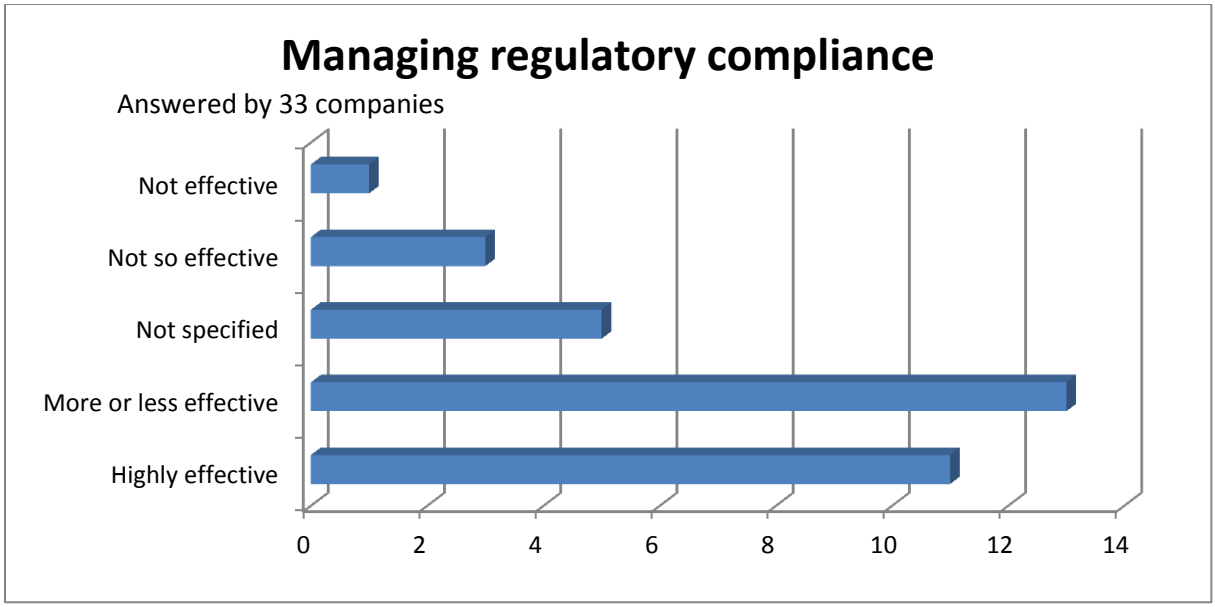


Figure 38. Managing regulatory compliance

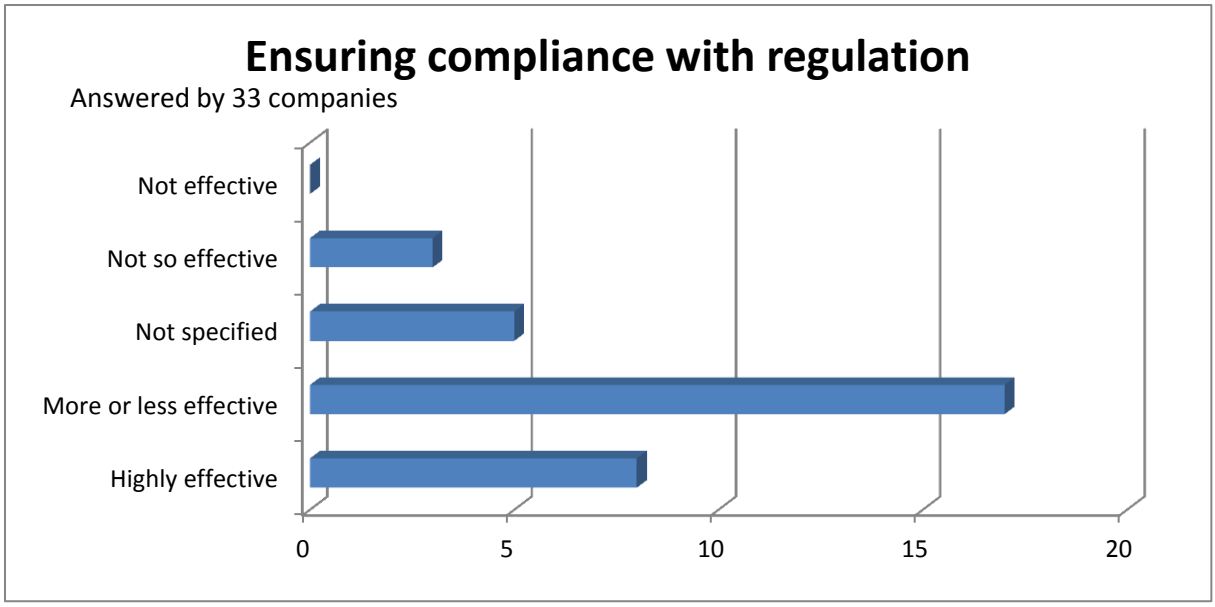


Figure 39. Ensuring compliance with regulation

1.11. Barriers

Associated with the effectiveness on the previous statements, we questioned the barriers that companies had come across and which prevented effective risk management. As already mentioned before the greatest barrier is the implementation of risk management in the corporate culture, 25 per cent of the companies state this as the most significant barrier. In declining order of significance we got the lack of support from senior management, which counts for 18 per cent, the shortage of available expertise and the lack of financial resources, both 14 per cent. The least chosen barrier is the ineffectiveness of tools and technology that are present in the company.

10 per cent of the companies had never thought of these barriers that prevented their risk management from being effective. Some entities clarified that they had faced other barriers. Implementing risk management in a decentralized structure is one of them. It has also been proven that it is difficult to deal with different risk practices in the business units. Not only the lack of financial resources could create a barrier but also the shortage of available people resources with responsibility for risk management.

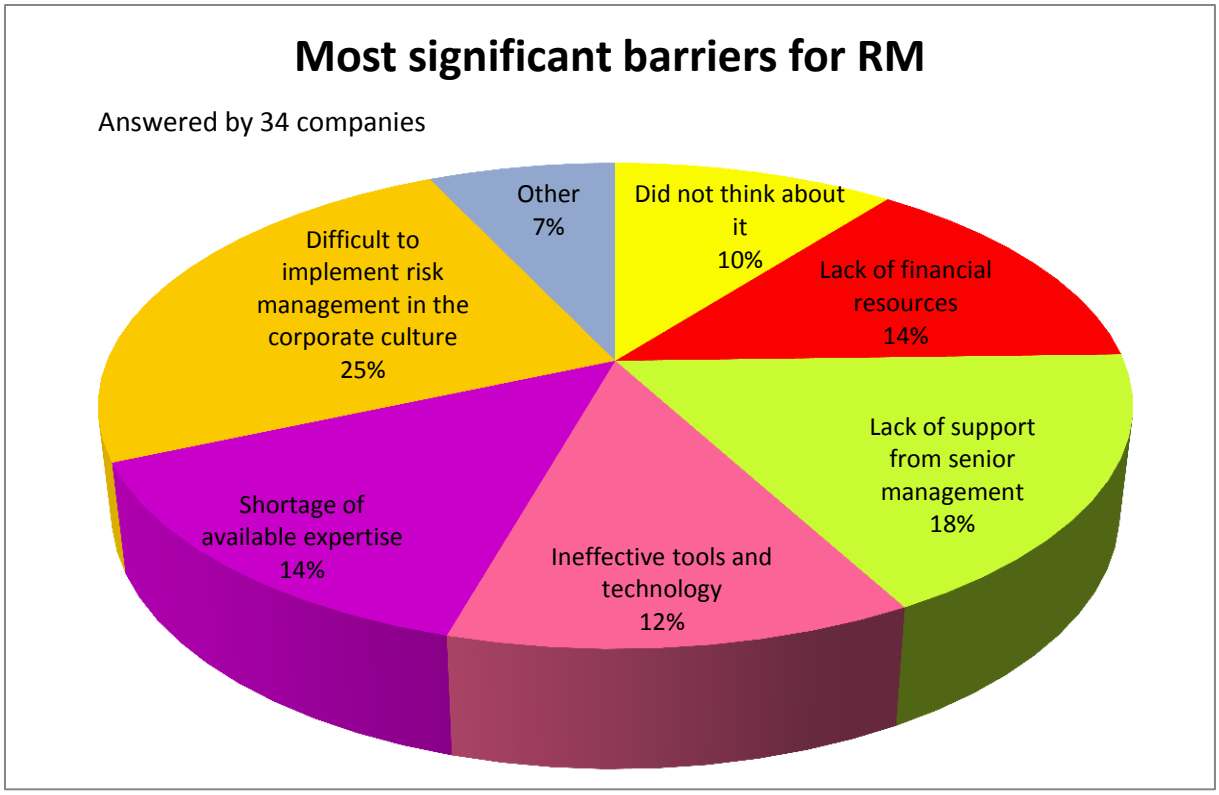


Figure 40. Most significant barriers for RM

1.12. Risk identification techniques

Further on, we were interested in the risk identification techniques that were used by the surveyed companies. By a general question we tried to derive which technique was the most applied one. Further, also the knowledge of techniques was investigated in a more specific question. The companies had the possibility to answer with "never heard of" and "not applied", "know the concept but not applied" and "know the concept and applied".

The most frequently used techniques are the interviews and self-assessments. When we asked which techniques the companies used, 71 per cent stated to use these interviews and self-assessments, when we specifically investigated this concept on the three-point scale, 82 per cent of the entities declared to know and to use this technique. This difference is partly due to the fact that the general question has been answered by 35 enterprises and the specific one by only 33 of them. Also in the specific question two extra companies state to use this technique. We need to notice that these differences also appear in the other risk identification techniques. There is only one company that claims to have never heard of these concepts.

Also popular is the brainstorming technique, in the general question 69 per cent declares to make use of this concept, in the specific question this is a 79 per cent. 6 per cent has never heard of this technique.

In the third ranking position, we found the risk questionnaires and the risk surveys, 46 per cent is implementing this concept according to the general question. 63 per cent in the specific question, this one has only been answered by 30 companies in comparison of the 35 of the general question. In this specific question an additional three companies seem to be using this technique. This concept also appears to be commonly known by at least 97 per cent of the respondents.

Subsequent we noted the event inventories, 40 per cent is making use of this technique, consistent with the general question. A 48 per cent concerning the specific question, which has been answered by 33 entities. This concept is less frequently applied and is not yet known by 21 per cent of the companies. We even included a description of this concept because it could occur that these event inventories are used but not known under this name.

In a decreasing order of occurrence, the next technique is the scenario analysis. This analysis is only been used by 31 per cent in the general question and by 43 per cent in the specific question. Again the specific question has only been answered by 30 companies. 13 per cent declares in this specific question to have never heard of this concept.

Finally, the last technique and therefore the least used one, is heat maps. 26 per cent says to be implementing this technique to identify risks. In the specific question this is 30 per cent but this deviation is only due to the number of enterprises who responded. In both questions 9 companies stated to use this technique. Also for this concept we provided a definition, still 40 per cent has never heard of this technique.

In the general question companies also got the possibility to inform us on other techniques they use to identify risks. Other techniques are value trees, risk taxonomy, Bayesian network and a tailor made risk policy. *Value trees* (Value Tree Analysis, 2002) are part of decision analysis. First the problem is structured, then the preference elicitation is made, this is where all the alternatives are being measured over a set of objectives. From this the recommended decision is derived, which ultimately leads to sensitivity analysis. *Risk Taxonomy* (Carr, Konda, Monarch, Ulrich, & Walker, 1993) is a technique to enhance the probability of the success of a project. It is a sort of scheme that defines the relationship amongst concepts concerning the same area of knowledge. Finally the *Bayesian network* (Jensen, 2009) is a graphical probabilistic model that helps reasoning under conditions of uncertainty. The network consists of a set of variables, nodes and the relations between them are directed by arrows.

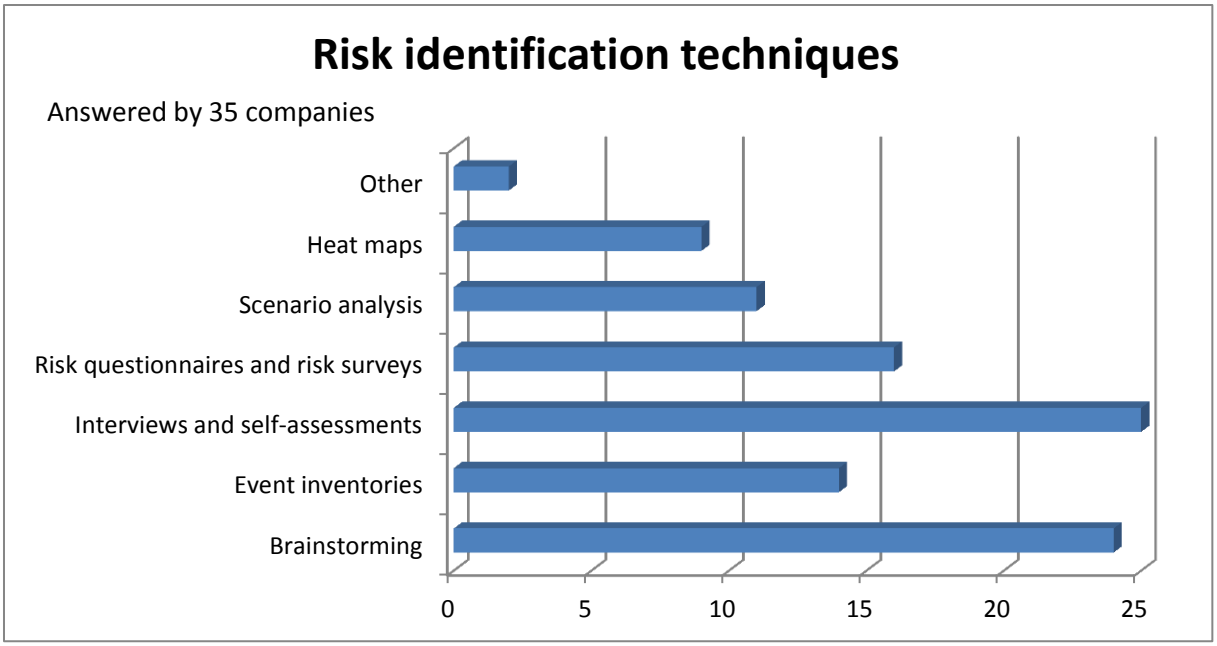


Figure 41. Risk identification techniques

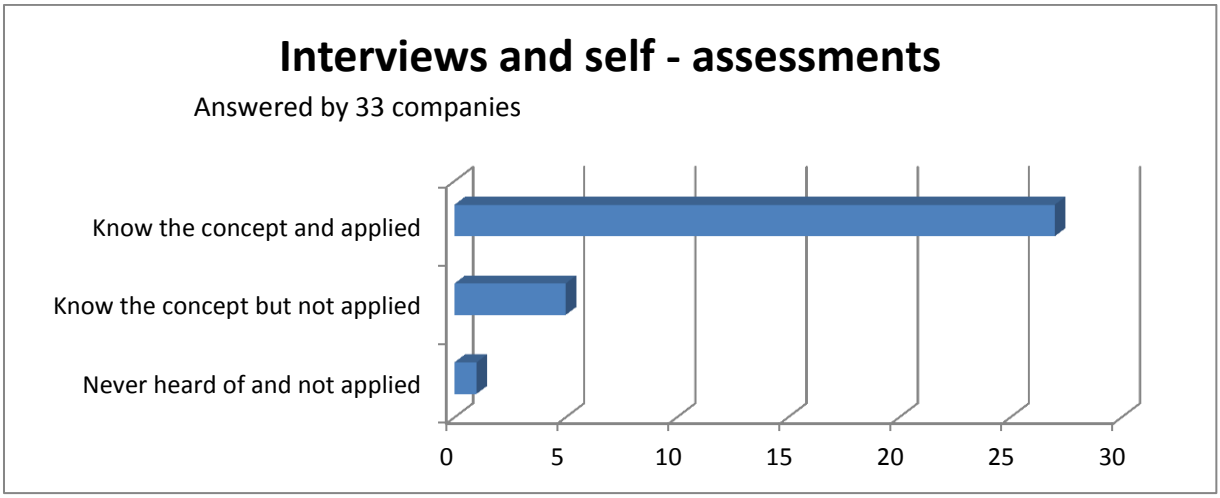


Figure 42. Interviews and self-assessments

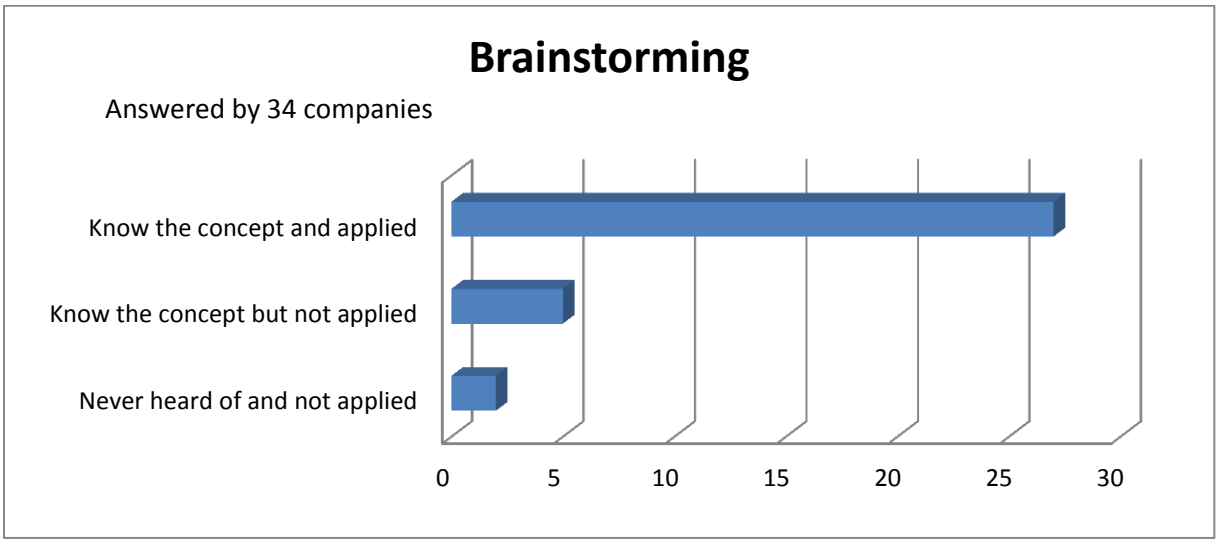


Figure 43. Brainstorming

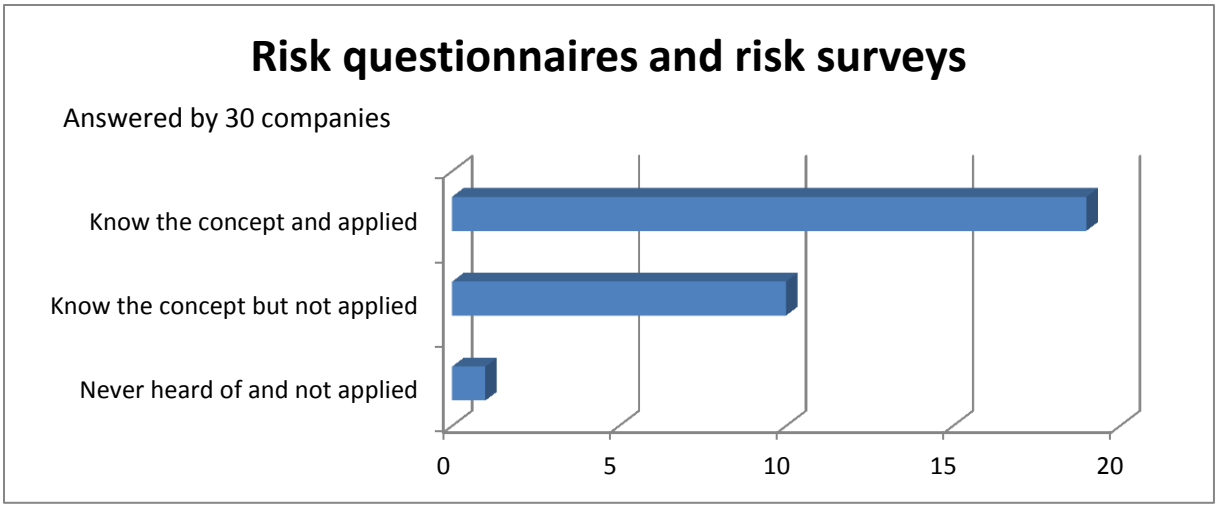


Figure 44. Risk questionnaires and risk surveys

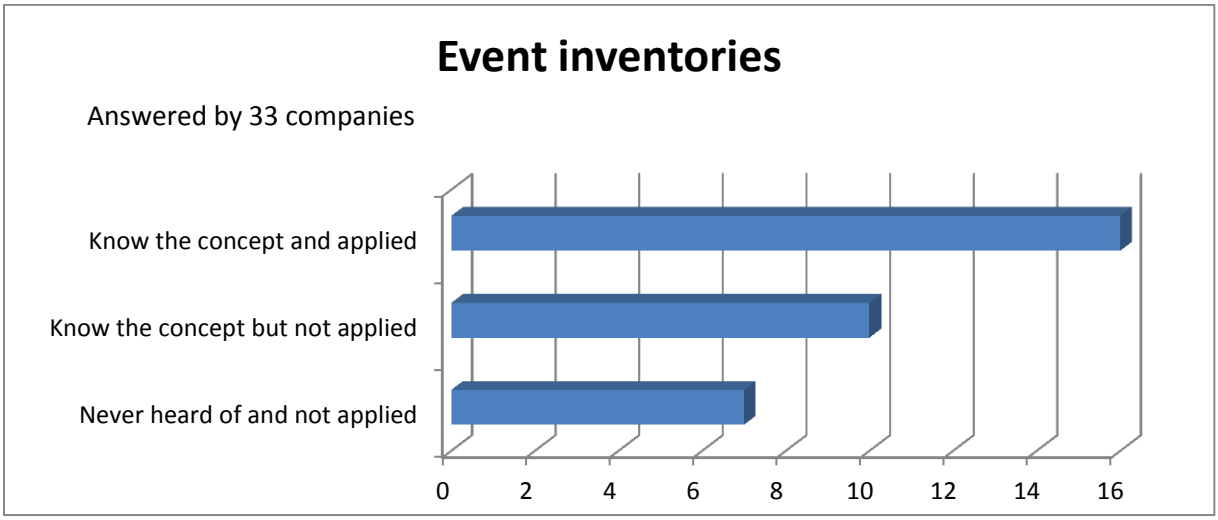


Figure 45. Event inventories

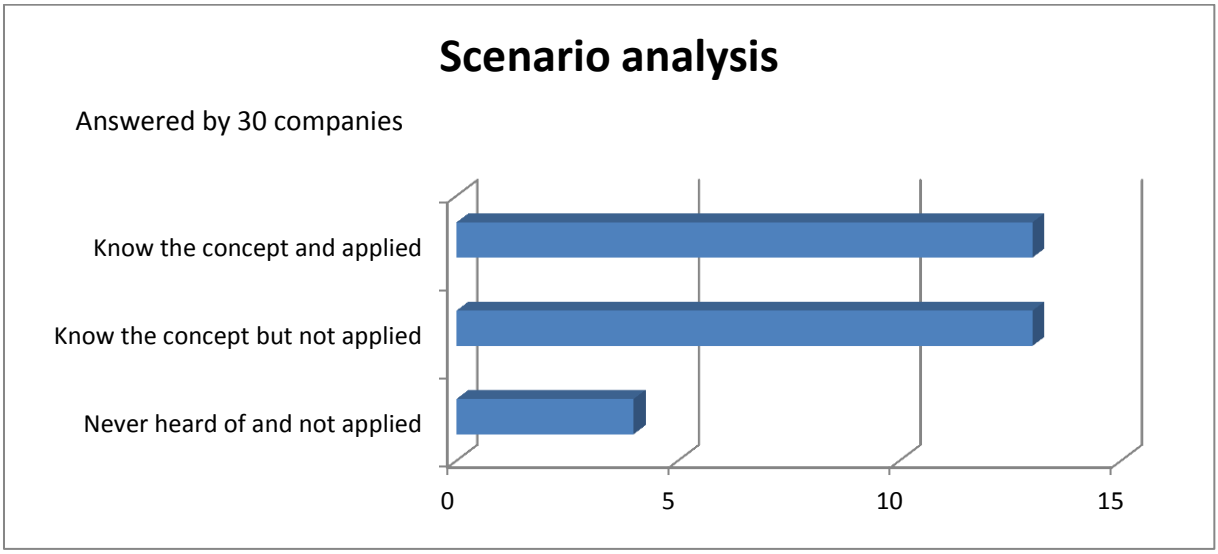


Figure 46. Scenario analysis

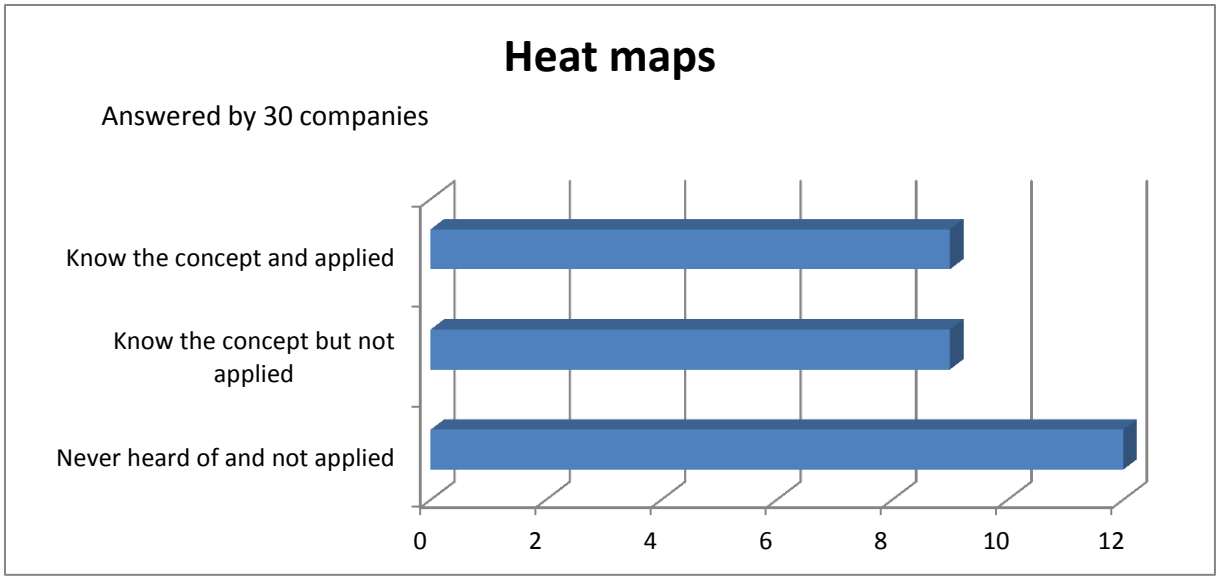


Figure 47. Heat maps

1.13. Standards used

In order to make the risk management process as smooth as possible, we would expect that most companies have adopted a risk management standard. When we asked this question, we offered 4 possibilities out of which the company could choose: no standard, COSO framework, ISO 31000 and a company specific standard. These options were based on our literature study where the COSO framework and the ISO 31000 standard are being described thoroughly. 39 organizations answered this question which gave us some interesting results.

14 organizations are using their own standard, followed by 13 companies that choose the COSO option. The ISO 31000 standard comes in last with only 4 companies and 8 companies claim they do not use any standard at all. An important remark is the fact that the companies were allowed to choose more than one option, depending on their situation. When we separate the companies that have checked more than one standard from those that have not done this, we notice that the classification is still valid. 11 enterprises use solely their own standard, 8 chose COSO and only 1 company marked the ISO 31000 standard as their only standard.

When we look at the combinations that the companies have chosen, we see that all possible combinations with COSO are being used. This leads us to the conclusion that when a company has its own standard, it will be using this solely, more than it would solely use COSO. When an organization uses COSO, in 40 per cent of the cases it will be using this in combination with their own standard or with ISO 31000. We also notice that in our sample of the Belgian companies, the ISO 31000 standard has not yet been intensively used. Since these are companies that are actively involved with risk

management, hence their membership with Belrim, we can state that the ISO 31000 standard will not be used a lot either in other companies in Belgium.

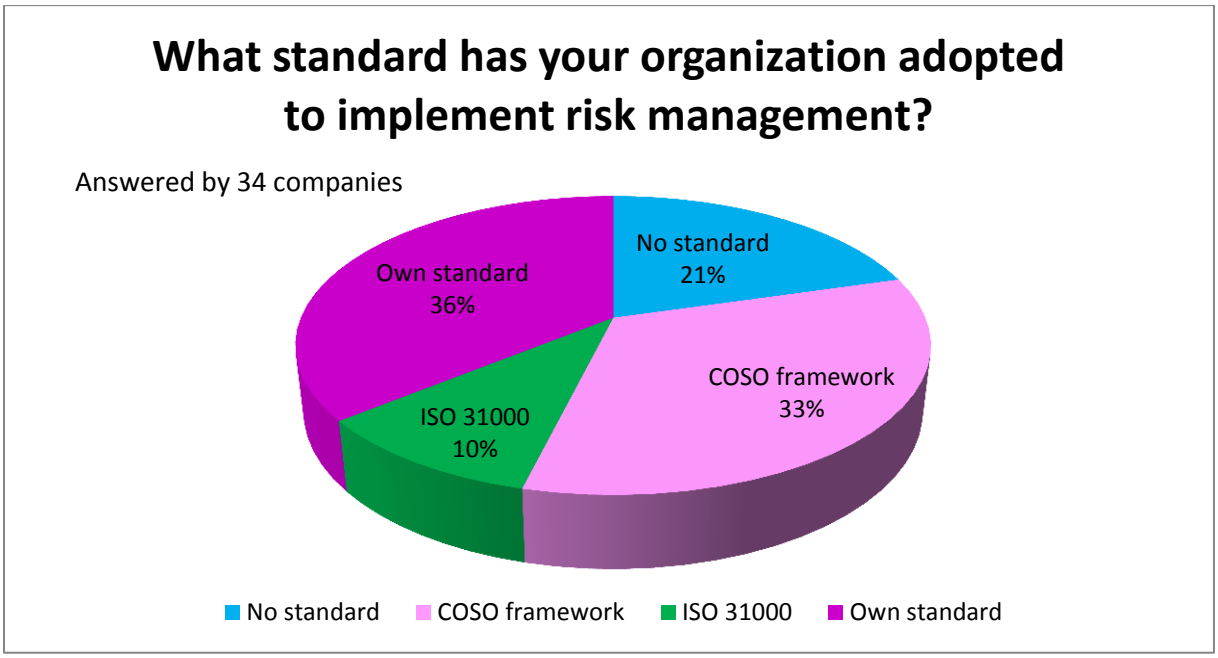


Figure 48. What standard to implement risk management

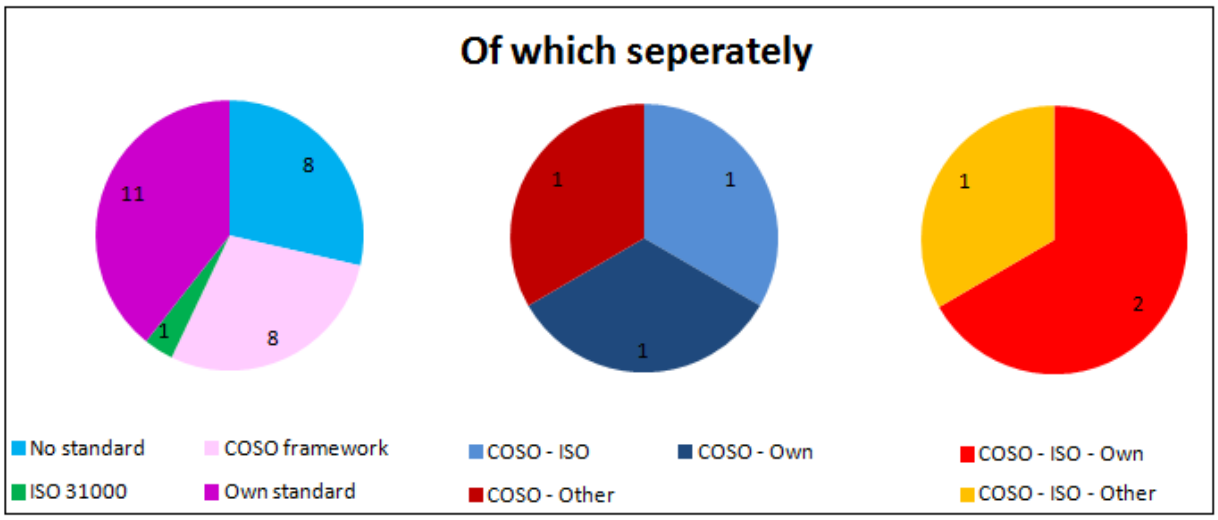


Figure 49. Separate applied standards

1.14. Investments in risk management

Since most, if not all, companies are involved with risk management in one way or another, it would be interesting to know how this engagement would be reflected in numbers. In view of obtaining this rather sensitive information, we asked to express this as a percentage of the companies' balance sheet total. The category of the zero to five per cent is by far the biggest category chosen. 23 companies of our sample of the Belgian companies choose this option. We would expect that our surveyed companies have an answer in the lowest category since this would already reflect a high investment.

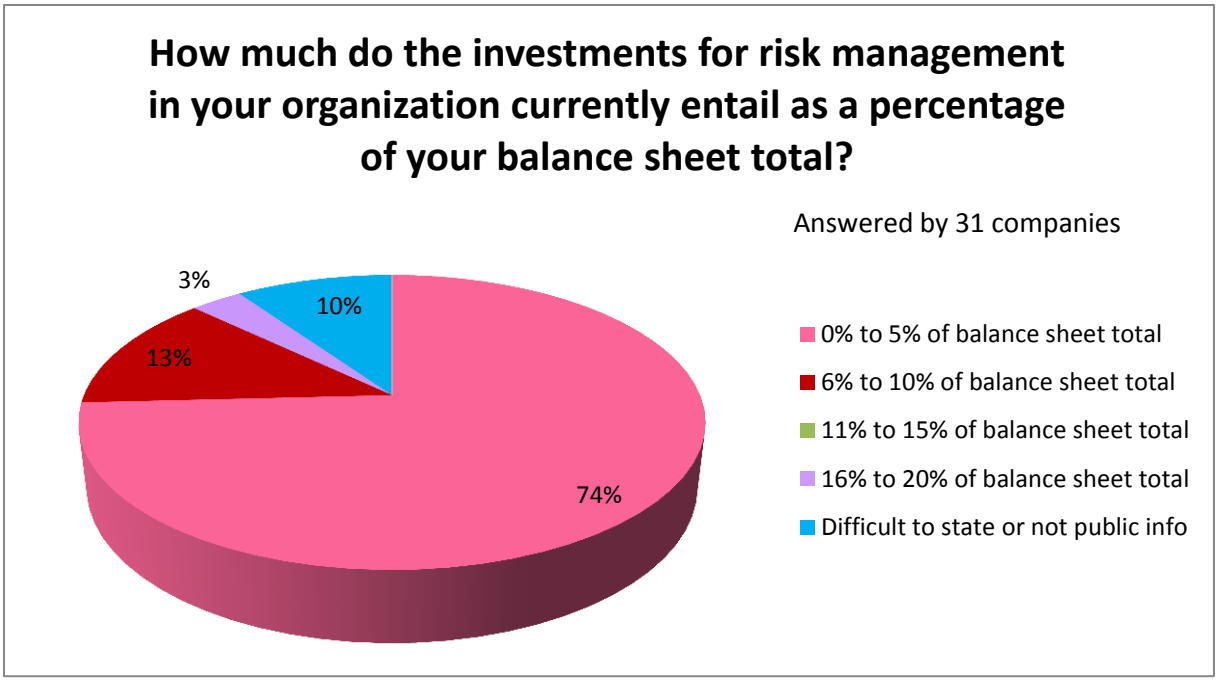


Figure 50. Investments in RM

1.15. Future challenges

Finally we would like to get some insights in the main future challenges for managing risk. The main challenge seems to be the development of a company culture with risk awareness, although 64 per cent of the companies already stated to be highly or more or less effective in the implementation of a risk culture. The second challenge is the alignment of risk management with the overall business strategy, which seems still a challenge in 28 per cent of the enterprises. Even though 60 per cent of the companies declared that they link risk management either highly effective or more or less effective to their corporate strategy. Further challenges are the improvement of risk reporting and the availability of sufficient budgets for investments in risk management. Other quoted challenges are the creation of a common risk culture, obtaining more objective measures for risk scores and implementing Business Continuity Management Plans (Senesael, 2009). These plans consist of instructions and procedures that need to be followed when the company faces a major risk or disaster. It should, in the best case, prevent that these events have an impact on the company's operations or at least minimize time lost in quickly reacting towards a crisis.

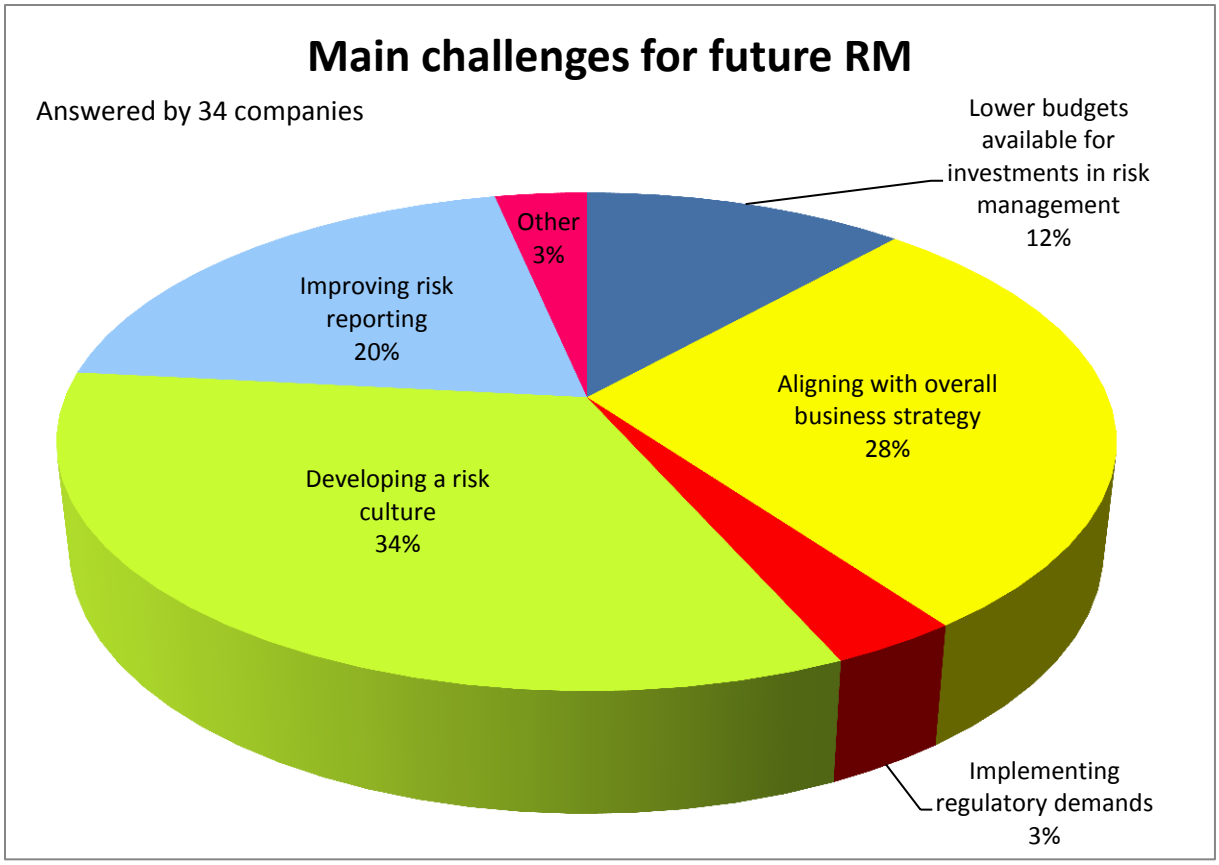


Figure 51. Main challenges for future RM

1.16. Future investments in risk management

Not only would it be interesting to know how the risk management engagement of our surveyed companies are reflected in numbers, it would also be worth knowing how the future will look like for the investments in our well discussed topic. We asked our participating organizations how they expect that the total level of their investment in developing risk management capabilities, will evolve in the next two years. More than half of the companies answered that the total level would remain the same. 40 per cent expected a moderate increase of less than 20 per cent. There were two exceptions on this question. One company answered that they would increase their investment more than 20 per cent and another, more out of line than the first, answered a decrease of more than 20 per cent.

We can make a comparison with the Accenture report[6] on this question. They have asked their surveyed companies almost the same question, a year before we did. On their question, 83 per cent of the companies answered that their investments would increase in the next two years. In more detail, 62 per cent believes that there will be a moderate increase and the remaining 21 per cent

[6] The global Risk Management Study (Accenture, 2011)

foresee an increase of more than 20 per cent. The 'no change' option received 14 per cent of the choice of the companies.

When we compare those results with our answers, we notice that three times more of our respondents have answered that they do not forecast any change coming up in the next two years. This difference can be explained by a number of factors. First, in our survey were more sectors included than the one of Accenture. As mentioned in the beginning of our findings, we have had an answer of at least one company in 21 different sectors. The Accenture investigation reached ten industries out of which 3 industries are not in our sample.[7] Secondly, their survey was done globally. Our research was done specifically in Belgium which can give us different results than when we would have investigated risk management in more countries. Thirdly, the Accenture report was written in 2011, a year before ours. This can give us a history effect.[8] Fourthly, we can define that our surveyed companies are already involved in risk management, so when we see that they will not change their investment in risk management, this can be the result of their previous adequate investments in the subject.

This leads us to the conclusion that the answers on this question are a good representation of the members of Belrim, but perhaps not a good one of all other Belgian companies.

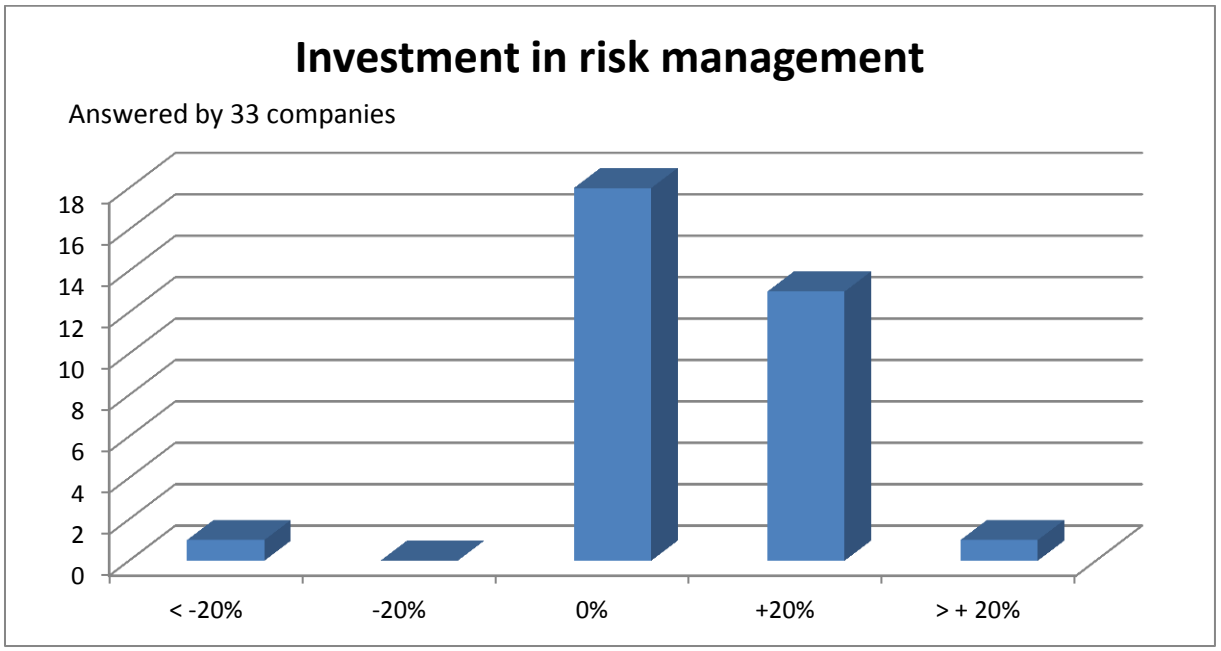


Figure 52. Investment in risk management

[7] Banking, Capital markets and life science

[8] History effect: Term often used in marketing when we speak of experiments or studies. The passing of the time between two surveys can cause a bias, so that we cannot say for sure that the change in the answer is a result of the changed attitude one has, or because of external factors that have appeared.

1.17. Opinions

The final topic of our enquiry dealt with three opinion-questions. We were interested to know what the ongoing thoughts were about the role of risk management in the companies. Our first question resulted somewhat scattered across the five answering possibilities.

We presented our respondents with the following statement: 'Risk management in our organization does not play a big enough role in identifying and assessing opportunities'. Around 30 per cent more or less agrees with this statement, followed by approximately 21 per cent who totally agrees. This results in more than half of the companies that agree that risk management should play a bigger role in identifying and assessing opportunities in the organizations. 18 per cent more or less agrees and about 12 per cent totally disagrees, giving us 30 per cent of the respondents that say that risk management does already play a big enough role in identifying and assessing opportunities. On this statement 18 per cent had no opinion.

The next topic of opinion was about the economic downturn. We wanted to know whether organizations had spent more attention on risk management due to the economic climate. Again, the answers showed no similarity with each other. About 36 per cent, of the 33 companies that answered this question, more or less agreed that it was because of the recent crisis that risk management had increased in importance. 9 per cent totally agreed that it was only because of the economic downturn that the risk management in their companies had received more attention. This results in 45 per cent of our respondents that admitted that their risk function had increased in importance as a result of the economic downturn. On the other hand, we have 24 per cent that more or less disagrees and 12 per cent that completely disagrees with our statement. This leads to 36 per cent of our surveyed companies that state that the economic downturn had not lead to an increased attention toward risk management. 18 per cent had no opinion. We can see that the answers do not provide a conclusive answer to this question, so we cannot conclude whether the economic crisis has had its impact on risk management or not.

Our last assumption the companies had to decide on, is a follow up on the previous one. We stated that risk management is likely to decline again in importance when the crisis is over. Here we received a more explicit answer. 40 per cent totally disagreed and 24 per cent more or less disagreed, which gives us 64 per cent votes for the 'no-camp'. However, still 21 per cent of the companies agrees that there was only more attention towards risk management due to the economic downturn. A negligible 3 per cent (1 company), totally agrees on this statement. 12 per cent had no opinion.

We can safely say that of the 45 per cent that said on the previous statement their risk function has increased in importance because of the crisis, only 33 per cent will let their risk management decline

again. The other 66 per cent has no intention to stop doing risk management when the good times return. The other 2 companies that will let their risk function decline in importance, more or less disagreed on the previous position.

As a conclusion from the last two statements: the companies that did not let their risk function increase due to the economic crisis, will also not let it drop when good times return. This can be because their risk management is already good or because they did not do anything with their risk function. Because our sample stems from the membership list of Belrim, we would agree to the first possibility. Also, when their risk function has inclined in importance, companies will not be likely to let it decline again when the crisis is over.

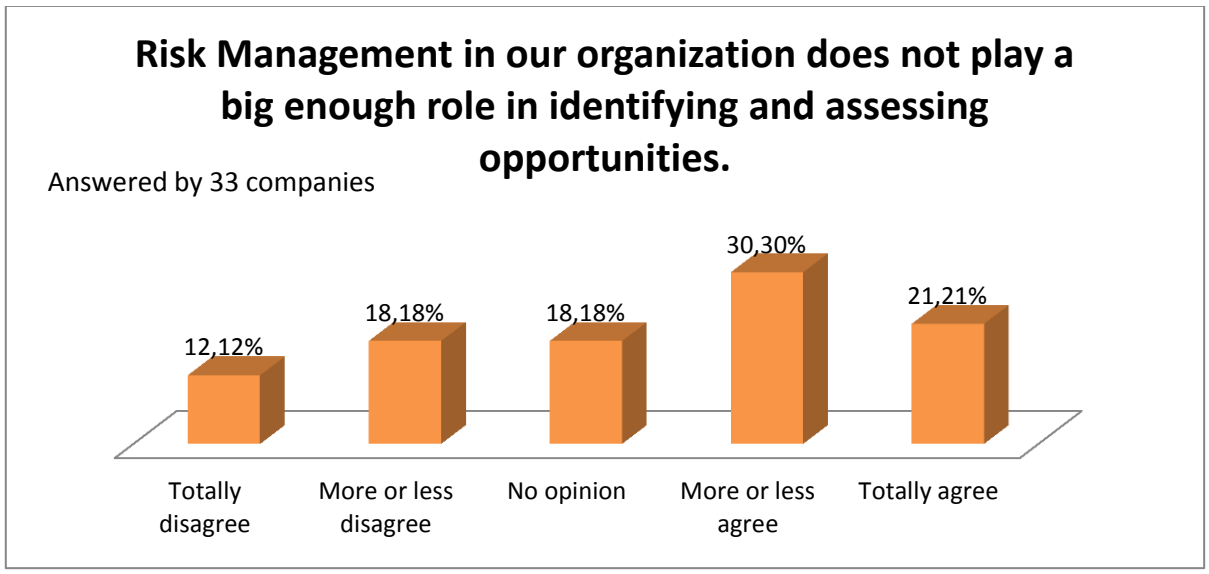


Figure 53. RM and its role in identifying and assessing opportunities

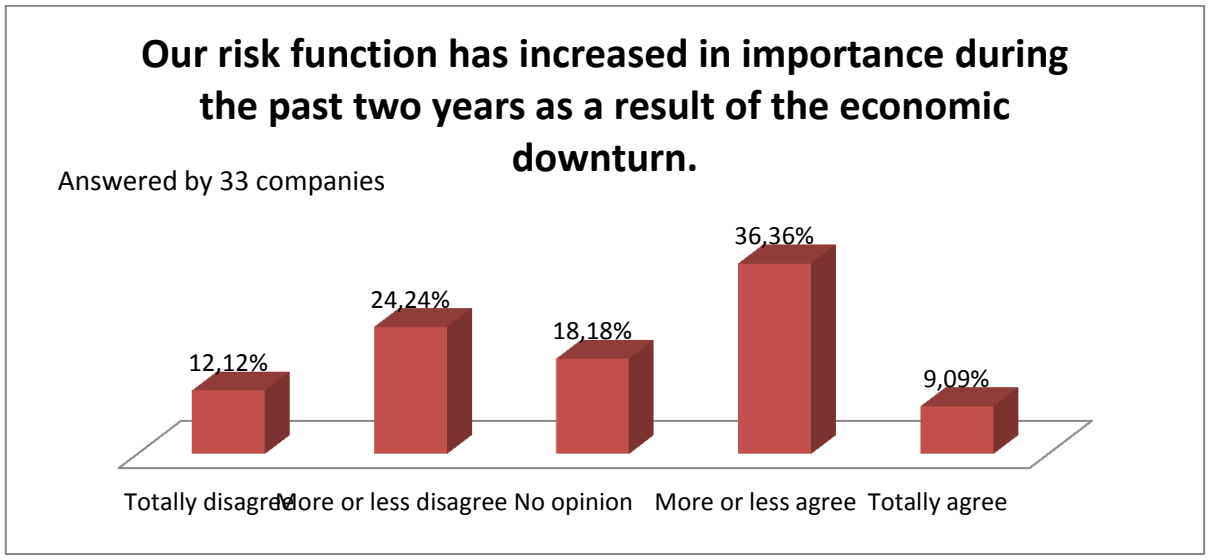


Figure 54. RM and economic downturn

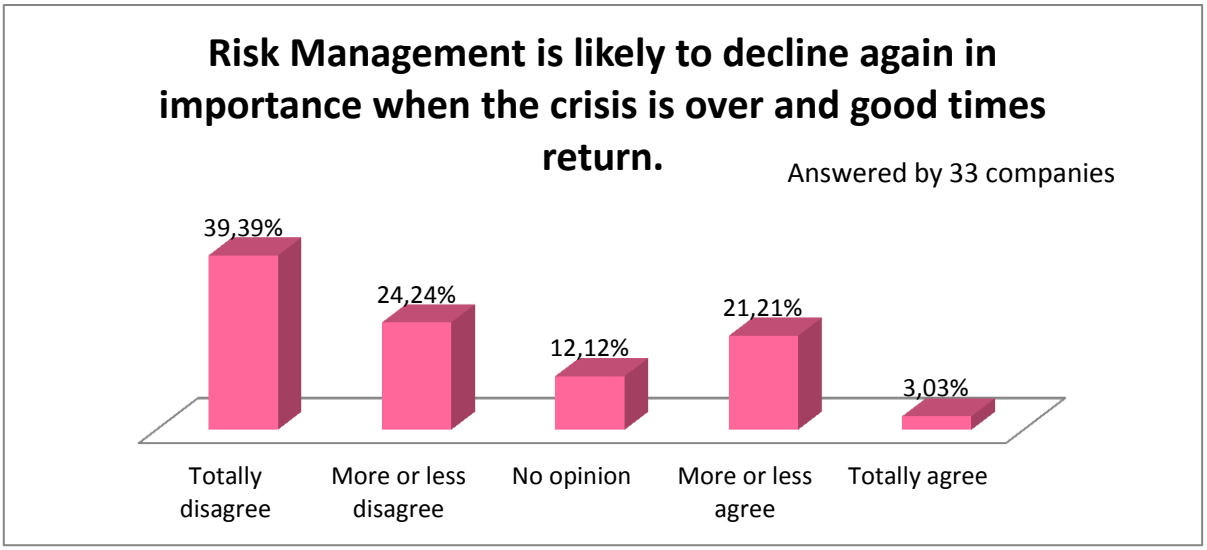


Figure 55. RM after crisis

Conclusions from empirical research

After looking into the theoretical part of risk management, we can give the reader a well-informed conclusion from our main empirical findings. This because we have examined the explained concepts, processes and techniques, which we have learned in the theory, in practice. A remark is in place; the conclusions we make in this section can be expanded to the companies in Belgium who are already involved with risk management, but caution is required when applying these results to all Belgian companies.
We advise the reader to look into our empirical research part for a more complete overview of our results.

The first topic we examined was the impact of the law of April 6, 2011 which requires that the main features for risk management should be recognized in the annual report. This effect can be found in more attention towards risk management and the better monitoring of existing standards and procedures. However, a fairly large part of 40 per cent answered that there was no impact. This can be explained by the ignorance of the law and the requirement of being listed. As an example of this law in practice, we saw that our second interviewed company has a section in its financial statements about their risk management. But, this company also claimed not to have an impact of this new requirement.

Closely linked is the awareness of the guidelines of the Commission of Corporate Governance to simplify the requirements of the new law. These are not commonly known so there is a need to give these directives more attention in the nearest future.

The implementation of Enterprise Risk Management Programs is currently not being done in 25 per cent of the companies. This in contrast with the fact that almost all organizations perform steps to identify or analyse risks. In the first visited company, we were given good examples of what the Risk Management Process means for them. They used a step based process containing 6 steps which we described thoroughly in the case study. Also the second visited company has a working Enterprise Risk Management program, however not as formal as the one of the first company. With respect to the ERM programs, we can conclude that the theory is being widely used and is certainly not behind on practice.

When looking deeper into the risks subjected to the ERM programs, the risk that is perceived as having the biggest influence on the sector of every company and on the individual company, is the operational risk. Companies also state this one as being the most frequently measured. An attentive

reader may have noticed that the compliance risk is knocked down from its first place when comparing our results with the Ernst&Young study (Ernst&Young, 2010) from our literature review.

Next topic of discussion included the tools and techniques companies use for identifying risks. The ones that companies use the most and therefore are most familiar with, are the interviews and self-assessments and the brainstorming technique. Heat maps are not commonly known and could be useful in the future turbulent economic environment. We did see an example of the implementation of heat maps in both visited companies.

Another conclusion that cannot be missed, deals with the use of COSO, ISO 31000 or a company specific standard. Most companies have an own risk management standard or use the COSO model. The ISO 31000 seems not to be commonly known or popular in our sample. We also notice that these standards can be used in combination with each other and as such, it is always the COSO framework combined with another standard. In our case studies, we also found the use of a company specific risk management standard and the COSO model.

Also interesting to know are the external factors that trigger risk management in an organization. The major ones are the legal requirements and compliance.

The question about who is responsible for managing risks, revealed that the line management is mostly seen as being responsible for risk management, closely followed by the Chief Risk Officer. These results are almost completely in line with the literature. There was stated that companies give responsibility to the Chief Risk Officer or when there is no Chief Risk Officer, organizations give more responsibility to their executives. We did however see that even when there is a Risk Officer, sometimes these persons are not pointed to as the responsible person for risk management. We can also conclude that companies do not give the internal audit a role of responsibility concerning risk management which is again more or less in line with the literature. There it was stated that it is important for the internal audit to focus on its core activities, which are not specifically situated in the risk management area.

The most important objective of the risk management function is to make it possible to take better managerial decisions. But, in contrast, the risk management function is expected to have the most meaningful contribution in addressing stakeholder concerns.

The most important barrier for effective risk management is the difficulty to implement risk management in the corporate culture, although companies rate themselves as more or less effective on linking risk management to the corporate strategy.

The majority of the companies expect their investments in risk management to remain the same in the coming two years. The largest part of them invests between 0 and 5 per cent of their balance sheet total in risk management.

Our last but one conclusion deals with the opinion of the companies about the economic downturn. We can conclude that in most of the companies, risk management was not being affected by the economic climate. In the organizations where this was the case, it was a positive influence of giving more attention to risk management.

Finally as our last finding, we compared the last section of the literature review, challenges for future risk management, with our own. Our results correspond with the last bullet of the challenges we found in literature. We see in practice that the main challenges for future risk management are the development of a risk culture and the alignment of risk management with the overall business strategy.

General Conclusion

The risk management concept, that can be described as a process that helps organizations address the risks that they come across when doing business, is commonly known in Belgian enterprises (The Institute of Risk Management, 2002). The risks are being classified in four categories, as we repeatedly saw in the literature. The categories that we adopted in our study and that are commonly used in practice, are the following: the financial, strategic, operational and compliance risk. However, the case studies that we conducted, showed that these four categories can be completed by some company specific divisions, like for example risk on corporate level or country level.

Most of the Belgian researched enterprises have an ERM program implemented that generally covers the basic steps of the risk assessment and risk treatment. This can be concluded based on our online enquiry and on the two case studies. Our research showed that risk identification, risk analysis and risk description are the most frequently performed steps. They are however closely followed by other steps like treatment, reporting and monitoring as a form of maturity. In the risk identification step, companies make use of some risk identification techniques. Some companies use these in a formal manner where every step is described and analyses are executed, which is what we saw in our first case study. The second case study on the other hand showed that this can also be done less formal based on brainstorming sessions and personnel interviews.

In the literature, as a frequently used tool for managing the identified risks, we found the heat map. This tool is a matrix that measures the impact and the probability of a specific risk on its own or in combination with other risks related to the same activity or project. Regardless of the attention given to this tool in business literature, still 40 percent of our questioned sample is totally unaware of the existence of this concept.

Most companies indicate the line manager as the person who is responsible for risk management in their company, a close second is the Chief Risk Officer. A striking conclusion in this area is that sometimes even when there is a CRO in the company, he is not designated as the responsible one. This is in contrast with the literature where the presence of a CRO would automatically lead to its responsibility in the area of risk management.

Deriving from the literature, the regulatory environment concerning risk management is dominated by the Committee of Sponsoring Organizations (COSO) and the International Organization for Standardization (ISO). The COSO framework is implemented in our two case studies, even though the second company is not a big supporter of this rather theoretical model. Based on our questionnaire's results we can conclude that 33 percent of the companies are using this COSO framework, but most

of the companies apply a company specific standard. The ISO 31000 standard on the other hand is not yet widely being used.

To come to conclusions in the area of authorities, we questioned the implementation of the new Belgian law of April 6, 2011. A majority of more than 70 per cent of the companies that answered, knew this new provision existed. We saw an example of the application of it in the second company. They described how they organize for risk management in their annual report. Important note on the implementation of this law is the condition that the company needs to be listed, which is an explanation for almost 40 per cent of the companies that see no impact of this new law.

The challenges for future risk management that were stated in our research are consistent with the ones mentioned in the literature. Companies still find it difficult to create an overall risk culture and to implement this in the company strategy.

Limitations

This research has its limitations that should be kept in mind. Since we cooperated with the Belgian Risk Management Association (BELRIM) to distribute our questionnaire, our sample does not represent the whole population of Belgian companies. We were able to draw conclusions about what the current state of affairs is, but we cannot say if the average Belgian company is managing risks.

It was difficult to draw general conclusions due to our rather limited sample size and the scattering of our participated companies across several industries made it also hard to generate conclusions about the separate sectors. We could only make use of basic analytical techniques since we needed to ensure the representativeness of our results.

Attention is also needed to some bias we noticed in the responses to certain questions, meaning that not all respondents were as consequent in their answers. It is however difficult to eliminate this sort of distortions.

Further research

As mentioned before, we conducted our survey mainly with the cooperation of Belrim members. It would be recommended to perform this study in Belgian companies who are not associated with the Belrim organization. This would give a clearer view on the ongoing state of implementation of risk management in those companies. Since it was our objective to research the state of affairs in risk management and the different procedures and techniques, we deliberately choose to enquire companies who were already engaged in risk management practices.

Further research could also emphasize on the role of Risk Officer. Our study prevailed that not in every company the risk manager is seen as the responsible for risk management even when there is such a function present. It could therefore be interesting to determine this function and its responsibilities within the organization. We advise to do this by means of another case study.

It is also recommended to investigate the evolution towards the implementation of the ISO 31000 standard. One can ask himself why companies do not implement this standard more often. The attention towards risk management is increased but the use of ISO 31000 remains limited. However, this standard can be very useful in implementing risk management.

Examination of risk management via depth interviews proved to disclose interesting information. It gives the possibility to ask open-ended questions and to compare the awareness and realization of risk management in different companies. Research within a particular industry or amongst sectors could both be worth investigating.

The last recommendation we make is to perform the same enquiry again next year in order to determine if risk management is or is not a phenomenon only caused by the current economic crisis. Repeating our enquiry would of course also be interesting to look for differences to see how the notion of risk management is evolving.

References

Accenture. (2011). *Report on the Accenture 2011 Global Risk Management Study.*

Airmic, Alarm, & IRM. (2010). *A structured approach to enterprise risk management and the requirements of ISO 31000.*

Belrim. (2012). *Belgian Risk Management Association*. Retrieved 4 2012, from <http://www.belrim.com/page/>

Bhimani, A. (2009). *Risk Management, Corporate Governance and management accounting: Emerging Interdependencies.* Elsevier.

Brown, I., Steen, A., & Foreman, J. (2009). Risk Management in Corporate Governance: A Review and Proposal. 546-558.

Carr, M., Konda, S., Monarch, I., Ulrich, C. F., & Walker, C. (1993). *Taxonomy-Based Risk Identification.* Pittsburgh, Pennsylvania: Software Engineering Institute.

Commissie Corporate Governance. (2011). *Interne controle en risicobeheer-richtlijnen.*

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management - Integrated Framework.*

COSO. (1985). *Committee of Sponsoring Organizations of the Treadway Commission*. Retrieved November 6, 2011, from <http://www.coso.org/aboutus.htm>

De Pelsmacker, P., & Van Kenhove, P. (2010). *Marktonderzoek - Methoden en toepassingen.* Pearson Education.

Deloitte invision. (2005). Global Risk Management Tool. Amstelveen, Nederland. Retrieved november 23, 2011

DG Internal Market. (2003). *Synthesis of the responses to the Communication of the Commission to the Council and the European Parliament "Modernising Company Law and Enhancing Corporate Governance in the European Union – A Plan to Move Forward" –.*

Ernst&Young. (2010). *The top 10 risk for business.* Oxford Analytica.

Fall guys - Risk Management in the Frontline. (2010). *The Economist*.

Financial Services and Markets Authority. (n.d.). *FSMA*. Retrieved September 9, 2011, from FSMA: <http://www.fsma.be/nl.aspx>

Frigo, M. L., & Anderson, R. J. (2011). *Embracing enterprise risk management.* COSO.

Institute of Management Accountants. (2007). *Enterprise Risk Management: Tools and Techniques for effective implementation.*

Jensen, T. B. (2009, September 28). Retrieved April 5, 2012, from University of Copenhagen: <http://www.prodstyr.ihh.kvl.dk/vp/2009/slides/BayesNet-I-6.pdf>

OECD. (2005, July). *Organization for Economic Co-operation and Development*. Retrieved November 6, 2011, from <http://stats.oecd.org/glossary/detail.asp?ID=6778>

PricewaterhouseCoopers. (2008). *A practical guide to risk assessment.* Pricewaterhousecoopers.

PWC. (2010). Risk Reporting and Risk Management Information.

Senesael, S. (2009, juni). *Business Continuity Management.* Retrieved mei 10, 2012, from FOD Binnenlandse zaken- algemene directie crisiscentrum: <http://www.crisis.ibz.be/documents/downloads/2009_BCM%20method_NL.pdf>

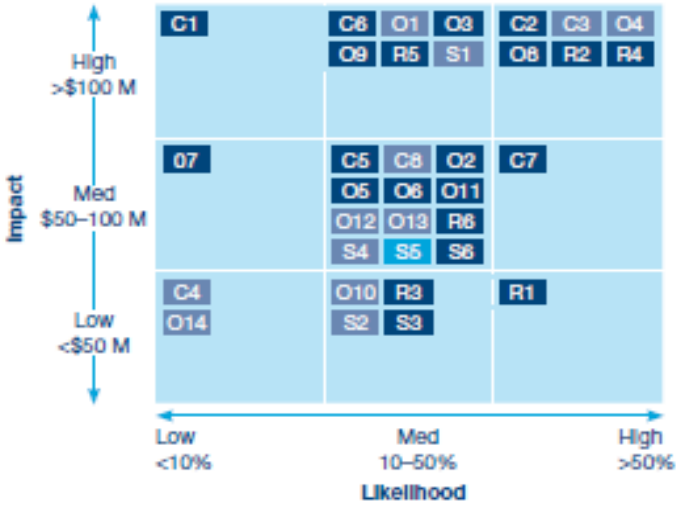
Steinberg, R., Martens, F., Everson, M., & Nottingham, L. (2004). *Entreprise Risk Management-Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The Institute of Risk Management. (2002). *A Risk Management Standard.*

Value Tree Analysis. (2002, April 30). Retrieved April 5, 2012, from <http://www.mcda.hut.fi/value_tree/theory/theory.pdf>

Appendices

Appendix 1: Risk Map (PricewaterhouseCoopers, 2008)



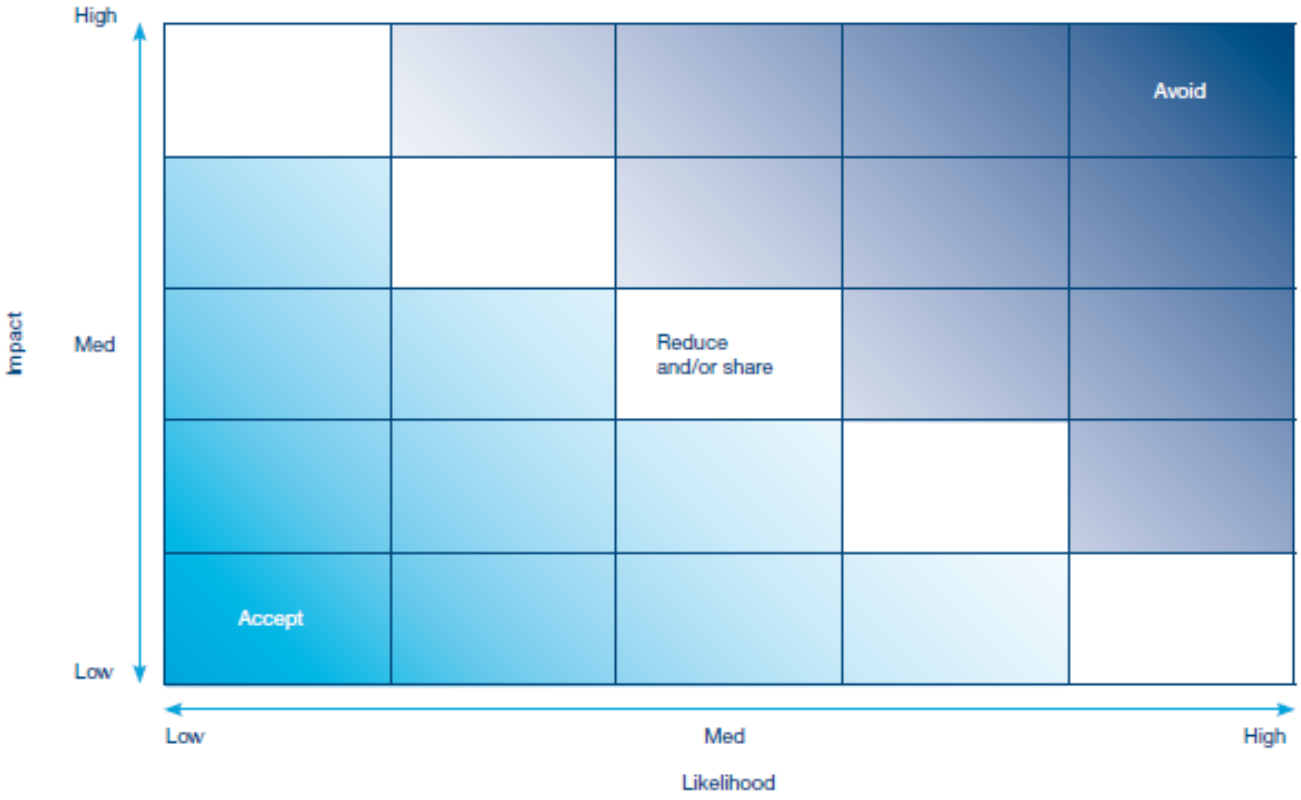
Increasing risk
Stable risk
Decreasing risk

Legend:
C – Compliance
O – Operational
R – Reporting
S – Strategic

Categories	Description
[C1] Compliance	Non-compliance with laws, regulations, or policies
[C2] Ethics and integrity	Fraudulent, illegal, or unethical acts
[C3] Intellectual property	Inability to enforce patents and trademark; infringement
[C4] Legal and disputes	Changing laws, liabilities, and commercial disputes
[C5] Product quality	Producing off-spec products
[C6] Product safety	Unsafe products
[C7] Regulatory	Changing regulations threaten competitive position
[C8] Tax	Failure to adequately support tax positions
[O1] Catastrophic loss	Major natural or manmade disaster; terrorism
[O2] Customer	Failure to follow customer preferences/needs
[O3] Efficiency	Inefficient operations
[O4] Engineering	Inability to design and manage facilities projects
[O5] Environmental	Environmental incidents or exceedances
[O6] Equipment	Plant equipment failure
[O7] Health and safety	Health and safety incidents harm employees
[O8] IT	Failure of IT systems; cyber attack
[O9] People	Lack or loss of qualified employees

Categories	Description
[O10] Security	Security breaches at company sites
[O11] Sourcing	Lack of access to key raw materials; failure of supplier
[O12] Supply chain	Failure of transportation and logistics network
[O13] Technology	Development of new, potentially disruptive technologies
[O14] Weather	Prolonged, adverse weather conditions
[R1] Commodity	Variability and increasing trends in commodity prices
[R2] Credit	Failure of customers or counterparties to perform
[R3] FX	Volatility in foreign exchange rates
[R4] Interest rate	Variability in interest rates
[R5] Investment	Financial market volatility impacts investments
[R6] Process design and execution	Failure in the design and execution of key management processes
[S1] Alliance	Inefficient or ineffective alliance, joint venture, affiliation
[S2] Capital adequacy	Lack of access to capital or liquidity
[S3] Competitive	Actions of competitors or new market entrants
[S4] Industry	Industry changes threaten industry attractiveness
[S5] Macroeconomic	Changes in broad economic conditions
[S6] Political	Adverse actions by foreign governments

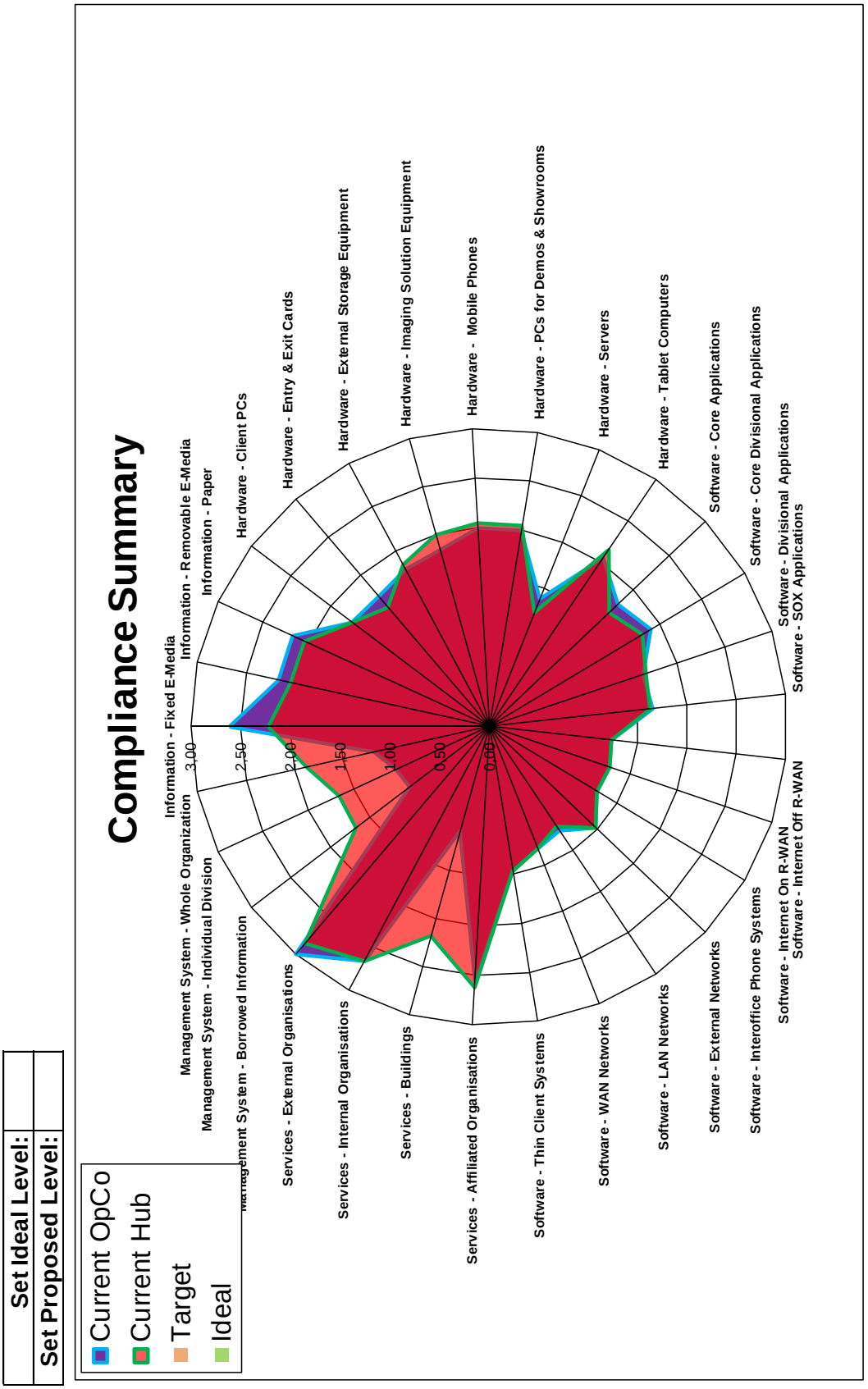
Appendix 2: Risk Response Strategies (PricewaterhouseCoopers, 2008)



Appendix 3: Questions interview

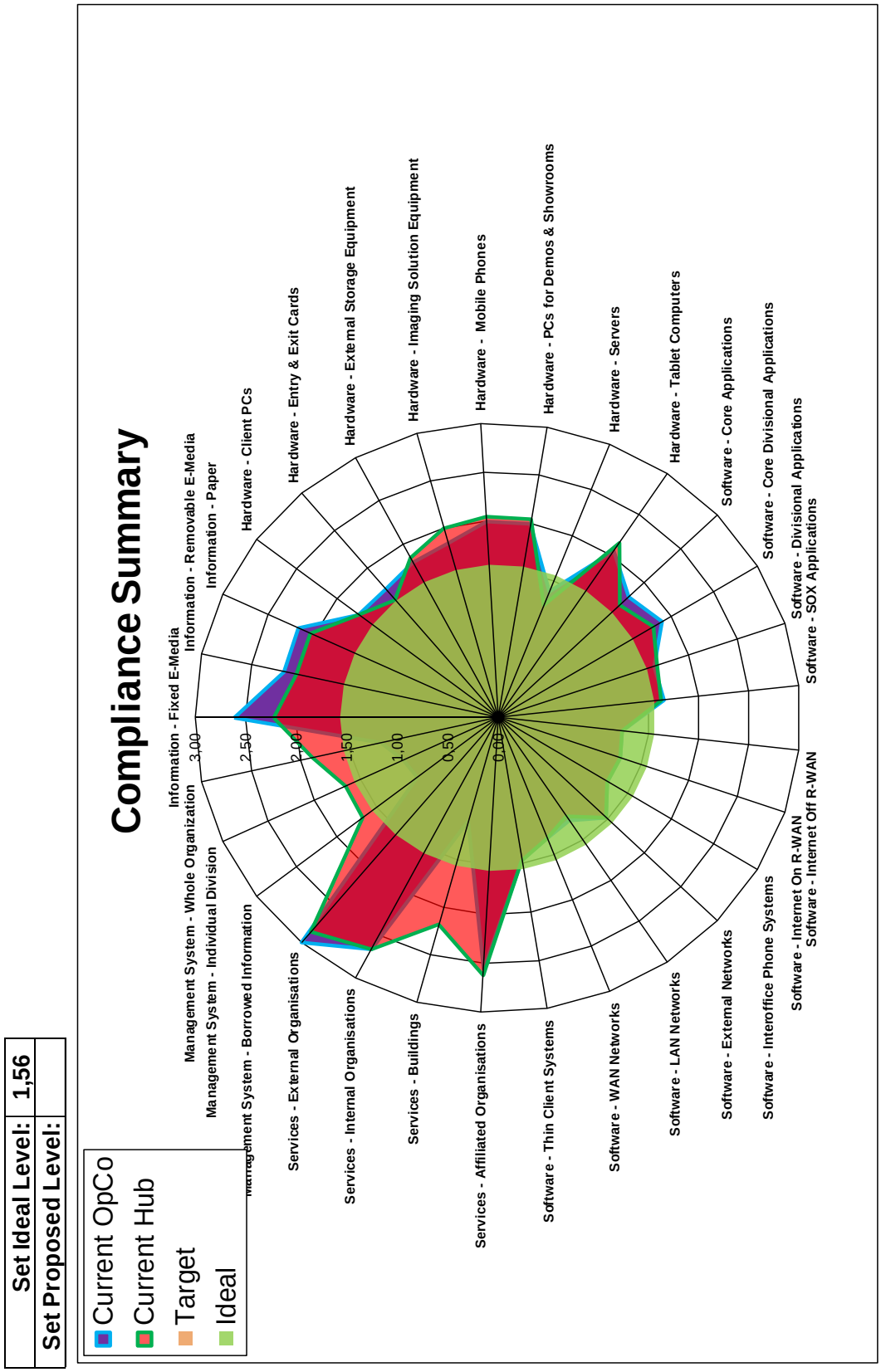
- Can you describe the risk management process that is used within the company and the different steps that are executed? (risk identification, risk description, risk estimation,…)
- Does your company uses the COSO framework or another standard/framework? (If the interviewees wants, with more information)
- What are the main risks for your company?
- What type of risks are being measured, managed and controlled?
- Which techniques do you use to identify risks (heat maps, brainstorming, etc) (Examples)
- Which are the procedures and tools to analyze these risks?
- Is risk management implemented in the culture and strategy of the organization?
- Who is responsible for risk management? (1 person, a team, all departments?)
- What about the communication of risk management towards the board of directors, stakeholders,..?

Appendix 4 a: 'Baseline objective summary'



Set Ideal Level:	
Set Proposed Level:	

Appendix 4 b: 'Baseline objective summary' – With ideal level

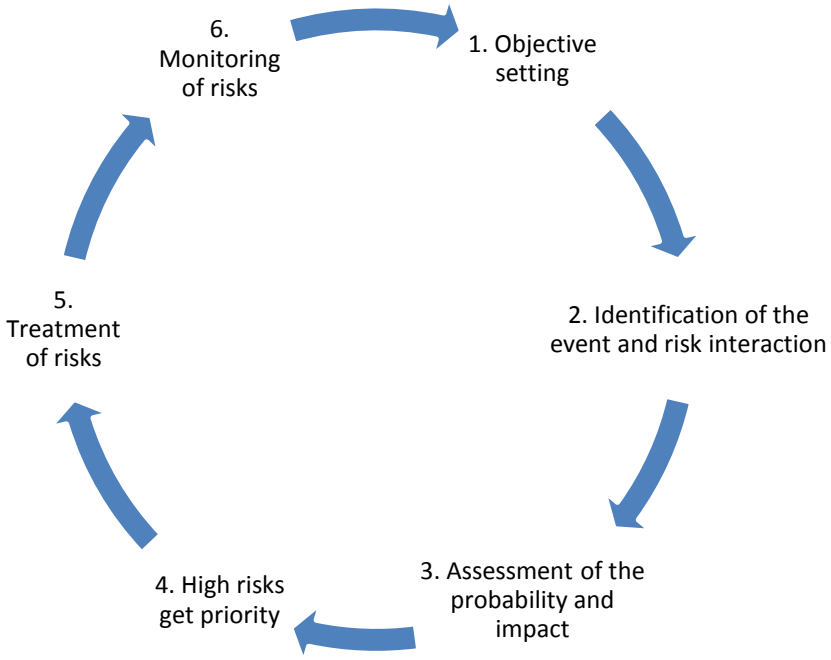


Set Ideal Level:	1,56
Set Proposed Level:	

Documentation Phase				
Process	**Sub-Process**	**Process Objective**	**Risks**	**Controls**
		What process should be executed	*Risks that obstruct process objective* *Risks that distort assertion*	*What controls should be implement*
SOXBE004 - D3 - V5.0	Process an order	Ensure that all contracts have accurately and completely been prepared and calculated by Business Administration to offer for financing with financing companies.	4. Incorrect STO (Service Take Out = coverage for the service expense of the contract, consisting of a fixed amount per copy, based on the size of the contract) has been recorded into UNIX, resulting in inaccurate revenue recognition regarding finance contracts.	12. If special STO's are used, these are approved according to the authorization database (called "Business Rules")

Risk	**Section/**	**Ref. No.**	**In-house**	**Relevant**	**Assertion**								**(COSO) Components**						**Control Character**			**Type of Controls**								
Level	**Person in charge**	**to Business Workflow**	**Standard or Manual**	**Accounts / Transactions**	*Mark "Y" in assertion applied*								**of Internal Control**									**Approval/Review**							
					Existence/Occurrence																	**Mapping of System Config. /Accounts**							
						Completeness																	**Report of Exceptional Items**							
							Valuation/Allocation						**Control Environment**										**Interface/Data Exchange**							
								Presentation/Disclosure						**Risk Assessment**									**Key Performance Indicator**						
									Rights&Obligations						**Control Activities**									**System access restriction**					
										Assets Safeguard						**Info. & Comm**									**Segregation of Duties**			
											Fraud Prev-						**Monitoring**									**Reconciliation**		
High *Mid* *Low*	*Practically worked Section/ person*		*Ref. of standards /manuals*	*Account Name or Description in Notes*															*Detective or Preventive*	*Automated or Human*	*Principal or Secondary*								
High	Service department + Business Administration - Order entry / Manager Product Marketing + SI and CP manager + employee BA		In-house	Sales, trade debtors, accruals, revenu recognition	Y	Y	Y	Y	Y		Y				Y		Y		Preventive	Human	Principal	Y		Y				Y		

Appendix 6: Roadmap



Appendix 7: Enquiry on risk management in non-financial companies in Belgium

Risk Management in non-financial companies in Belgium: A state of affairs

We would like to investigate the state of affairs on risk management. Your cooperation to our enquiry would help us to achieve a better evaluation of the current situation.

We ask about 10 minutes of your time to complete this questionnaire, which is strictly anonymous and we thank you in advance.

Laurien Van den Meerssche and Julie Van Heghe
(Master of Science in Applied Economics, Accountancy - University of Ghent)

Start

1. **In which sector does your company operate? (1 answer)**
(In case of a multi-business company please refer to the business activity with the biggest revenues)

- ○ Audit and Consultancy
- ○ Construction
- ○ Consumer Goods and Services
- ○ Energy
- ○ Healthcare
- ○ High Tech
- ○ ICT
- ○ Pharmacy
- ○ Public & social profit
- ○ Retail
- ○ Utilities
- ○ Other

2. **In what category is your headcount situated?**

- ○ 0 - 50
- ○ 51 - 100
- ○ 101 - 500
- ○ 501 - 1000
- ○ more than 1000

3. **Give an estimate of your company's turnover? (Only for the Belgian part)**

4. **What is your job title? (1 answer)**

- [ ] Accountant
- [ ] Finance Director
- [ ] General Manager
- [ ] Internal auditor
- [ ] Risk Officer
- [ ] Other

5. **Are you aware of the new requirements of the Belgian law of April 6, 2011? (1 answer)**
(Under the law of April 6, 2011 listed companies are obliged to mention their main features in the annual report. In this manner an attempt is made to a clearer understanding of the corporate governance of the company, and more specifically of the internal control and Risk management systems.)

- ( ) Yes
- ( ) No

6. **What has been the impact of this new law of April 6, 2011 on your company? (maximum 4 answers)**

- [ ] No impact
- [ ] More attention towards risk management
- [ ] More budget for risk management
- [ ] Better monitoring of existing procedures and/or standards
- [ ] New procedures and/or standards
- [ ] Other

7. **Are you aware of the guidelines that the Commission of Corporate Governance has worked out to simplify the requirements of the Belgian law of April 6, 2011?**

- ( ) Yes
- ( ) No

8. **Is your company currently using these guidelines in order to simplify the requirements of the Belgian law of April 6, 2011?**

- ( ) Yes
- ( ) No

9. **What are the biggest specific risks in your SECTOR? (maximum 3 answers)**

- [ ] Compliance risk
- [ ] Liquidity risk
- [ ] Market risk
- [ ] Operational risk
- [ ] Reputation risk
- [ ] Strategic risk
- [ ] Technical risks
- [ ] Weakening demand
- [ ] Other

10. **What are the biggest specific risks in your ORGANISATION? (maximum 3 answers)**

- ☐ Compliance risk
- ☐ Liquidity risk
- ☐ Market risk
- ☐ Operational risk
- ☐ Reputation risk
- ☐ Strategic risk
- ☐ Technical risks
- ☐ Weakening demand
- ☐ Other

11. **Does your company have an Enterprise Risk Management program?**
("Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite to provide reasonable assurance regarding the achievement of entity objectives.")

- ○ Yes
- ○ No

12. **Indicate which steps in the risk management process your company undertakes.**

- ☐ Risk analysis
- ☐ Risk identification
- ☐ Risk description
- ☐ Risk estimation
- ☐ Risk evaluation
- ☐ Risk reporting
- ☐ Risk treatment
- ☐ Monitoring
- ☐ None of the above

13. **Which risks is your company currently measuring? (multiple answers possible)**

- ☐ Business risks
- ☐ Credit risks
- ☐ Legal risks
- ☐ Liquidity risks
- ☐ Market risks
- ☐ Operational risks
- ☐ Regulatory requirements
- ☐ Strategic risks
- ☐ Technical risks
- ☐ Other

14. **Which of the following stakeholders have the strongest influence on your organisation's approach to risk management? (maximum 3 answers)**

- ☐ Banks
- ☐ Customers
- ☐ Employees
- ☐ Government
- ☐ Insurer
- ☐ Investor
- ☐ Management
- ☐ Rating agencies
- ☐ Other

15. **What are the main external factors that trigger risk management within your company? (maximum 3 answers)**

- ☐ Legal requirements
- ☐ Compliance
- ☐ Catastrophic event
- ☐ Pressure from the market
- ☐ Other

16. **Who is responsible for managing risk in your organisation? (You may indicate more than 1 answer)**

- ☐ Chief Risk Officer
- ☐ Finance department
- ☐ Internal audit
- ☐ Internal control
- ☐ Line management
- ☐ Other

17. **What do you think is the MOST important objective of the risk management function? (1 answer)**

- ○ Measuring and monitoring the most important risks
- ○ Ensuring compliance with regulation
- ○ Making it possible to take better managerial decisions
- ○ Implementing a risk culture
- ○ Other

18. **How would you rate the effectiveness of your organisation at the following activities?**

	Highly effective	More or less effective	Not specified	Not so effective	Not effective
Linking risk management with corporate strategy	○	○	○	○	○
Communicating risk information to investors	○	○	○	○	○
Managing regulatory compliance	○	○	○	○	○
Communicating risk management information to the board of directors	○	○	○	○	○
Implementing a risk culture	○	○	○	○	○
Ensuring compliance with regulation	○	○	○	○	○

19. **Where do you expect risk management to make the most meaningful contribution to your organisation? (1 answer)**

- ○ Compliance with regulatory requirements
- ○ Securing market share
- ○ Reputational advantage
- ○ Addressing stakeholder concerns
- ○ Other

20. **In the past year, what have been the most significant barriers to effective risk management in your organisation? (multiple answers possible)**

- ☐ Did not think about it
- ☐ Lack of financial resources
- ☐ Lack of support from senior management
- ☐ Ineffective tools and technology
- ☐ Shortage of available expertise
- ☐ Difficult to implement risk management in the corporate culture
- ☐ Other

21. **What will be the main challenges in the future for managing risk in your company? (maximum 2 answers)**

- ☐ Lower budgets available for investments in risk management
- ☐ Aligning with overall business strategy
- ☐ Implementing regulatory demands
- ☐ Developing a risk culture
- ☐ Improving risk reporting
- ☐ Other

22. **Which techniques does your organisation use to identify risks? (multiple answers possible)**

- ☐ Brainstorming
- ☐ Event inventories (These give an overview of all the possible risks within an industry and are used to give a basis for the brainstorm session.)
- ☐ Interviews and self-assessments
- ☐ Risk questionnaires and risk surveys
- ☐ Scenario analysis
- ☐ Heat maps ((This is a method to visualize the importance of certain risks. A heat map gives the advantage to look at every risk individually and in relation with others.)
- ☐ Other

23. **Are you familiar with the following techniques? (1 answer)**

	Never heard of and not applied	Know the concept but not applied	Know the concept and applied
Brainstorming	○	○	○
Event inventories	○	○	○
Interviews and self-assessments	○	○	○
Risk questionnaires and risk surveys	○	○	○
Scenario analysis	○	○	○
Heat maps	○	○	○

24. **What standard has your organisation adopted to implement risk management?**

- [ ] No standard
- [ ] COSO framework
- [ ] ISO 31000
- [ ] Own standard
- [ ] Other

25. **How much do the investments for risk management in your organisation currently entail as a percentage of your balance sheet total? (1 answer)**

- ○ 0% to 5% (5% included)
- ○ 6% to 10%
- ○ 11% to 15%
- ○ 16% to 20%
- ○ More

26. **What is your opinion on the following statements?**

	Totally disagree	More or less disagree	No opinion	More or less agree	Totally agree
Risk Management in our organisation does not play a big enough role in identifying and assessing opportunities.	○	○	○	○	○
Our risk function has increased in importance during the past two years as a result of the economic downturn.	○	○	○	○	○
Risk Management is likely declines again in importance when the crisis is over and good times return.	○	○	○	○	○

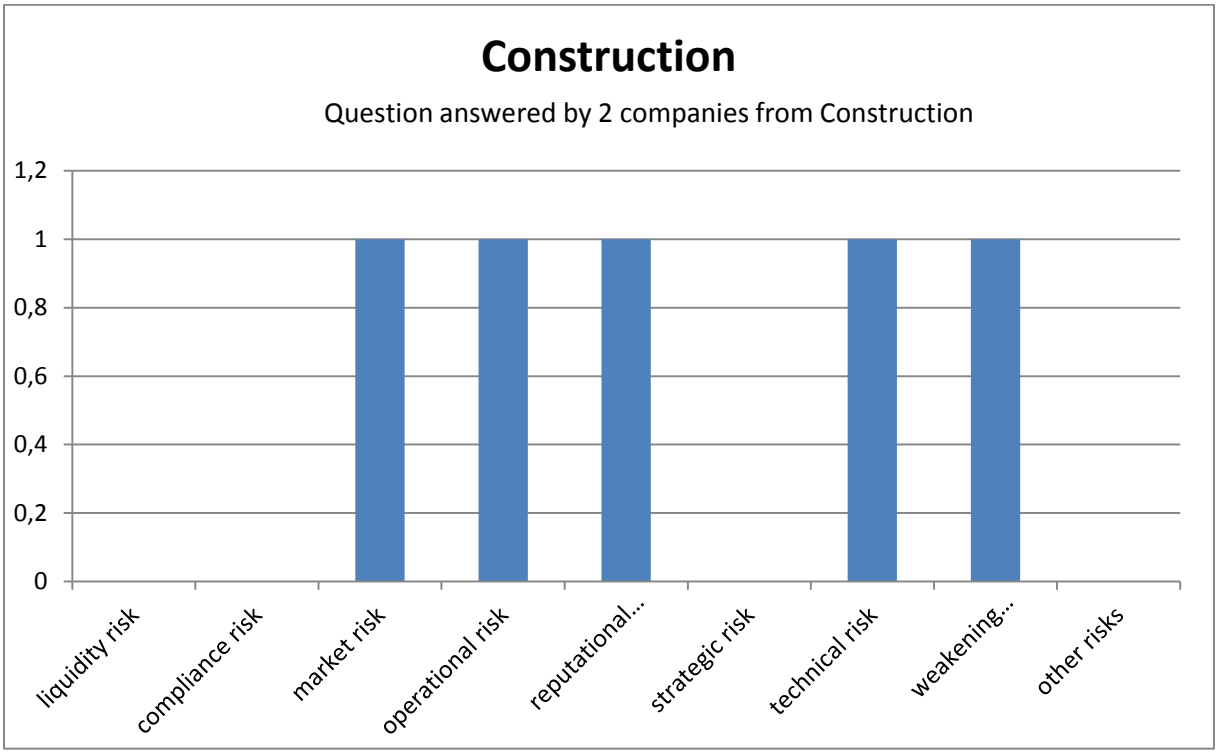
27. **Companies expect to invest in their risk management capabilities in the coming years. How do you expect that the total level of investment to develop risk management capabilities will involve in the next two years in your organisation? (1 answer)**

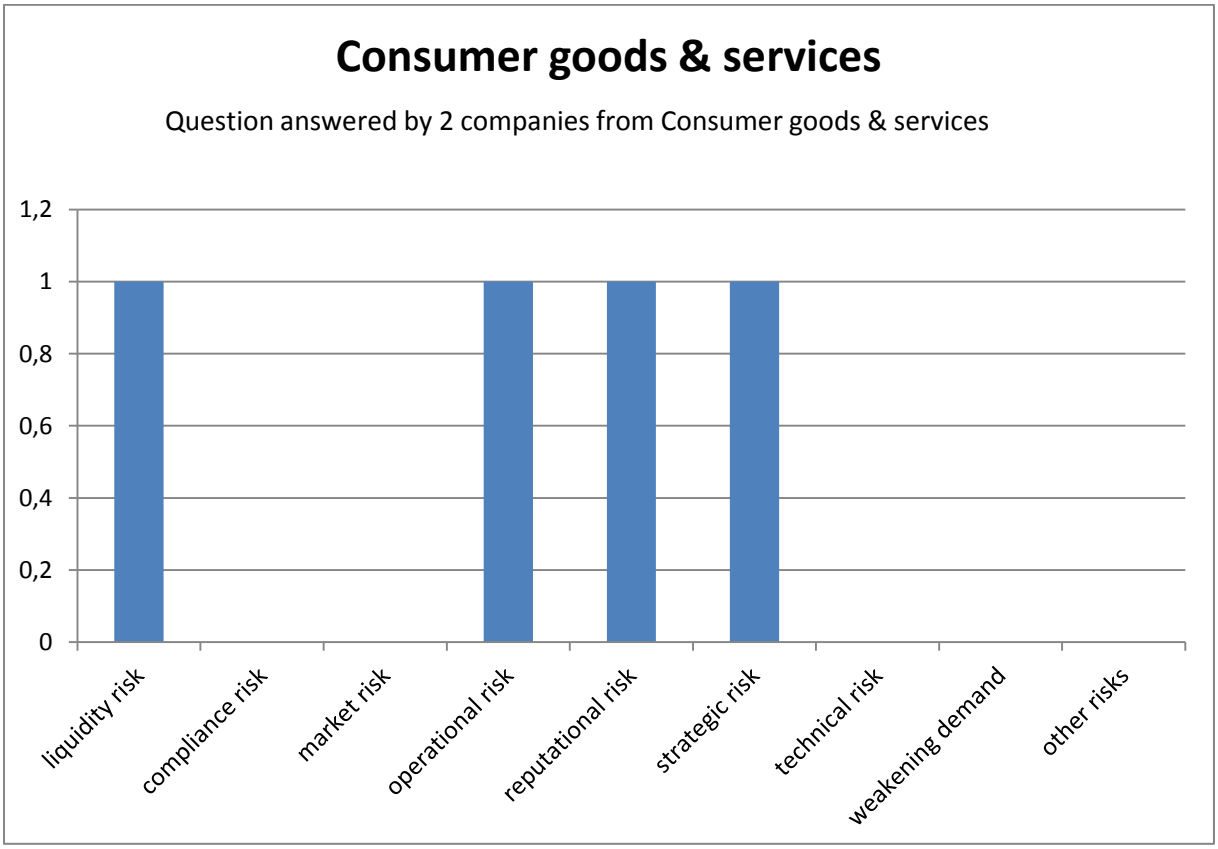
- ○ Significant decrease(-20% on the investment budget and more)
- ○ Moderate decrease(less than -20% on the investment budget)
- ○ No change
- ○ Moderate increase(less than +20% on the investment budget)
- ○ Significant increase(+20% and more on the investment budget)

Thank you for completing our questionnaire.

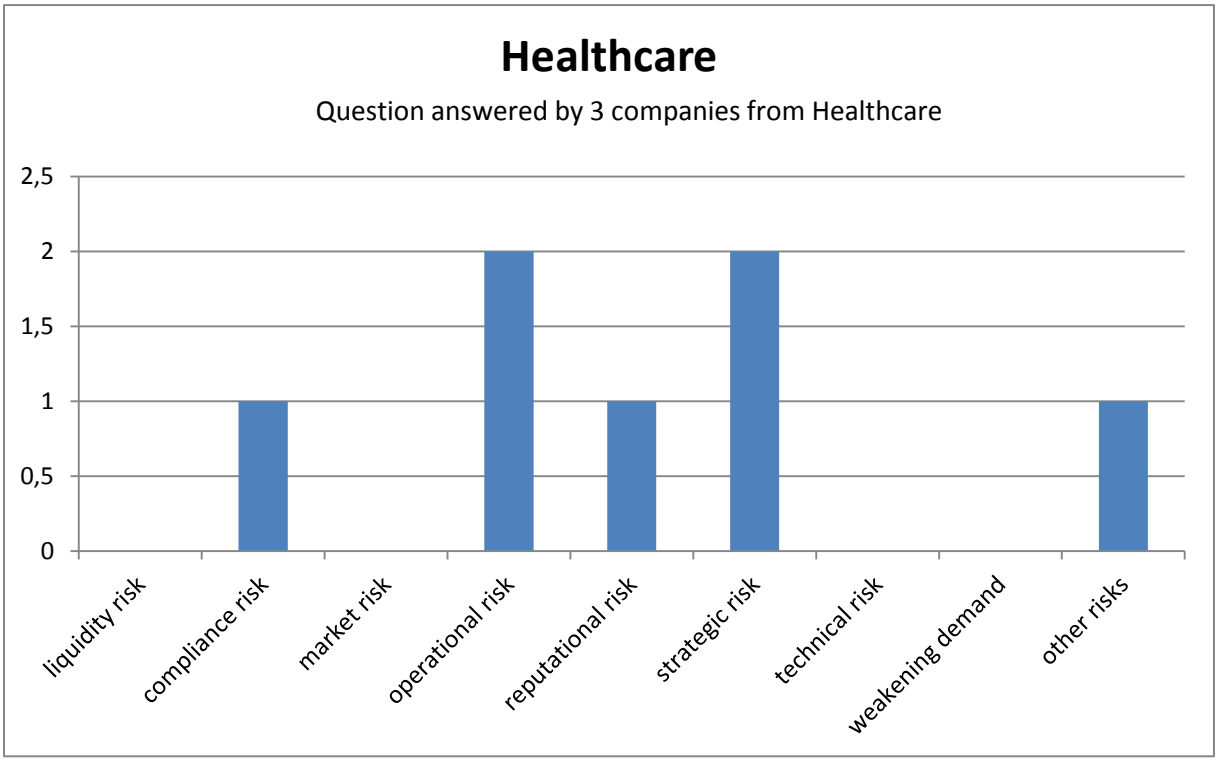
Laurien Van den Meerssche and Julie Van Heghe

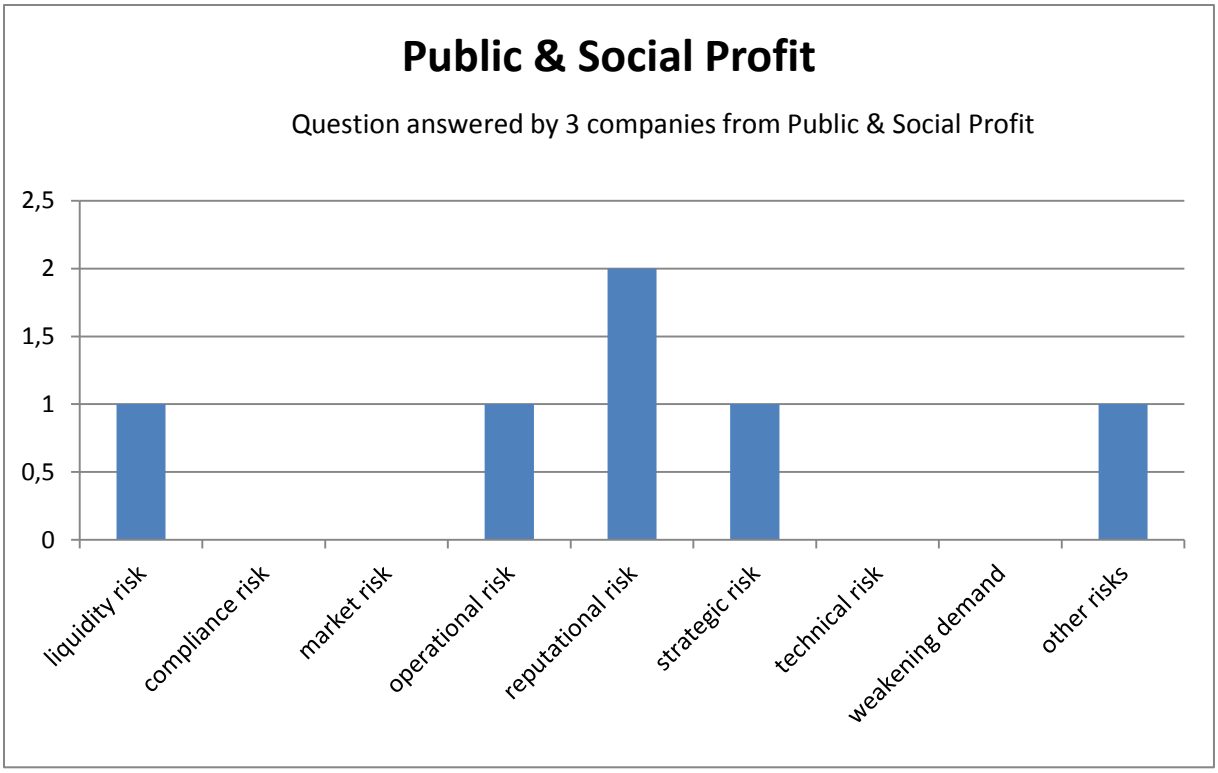
Appendix 8: Risk perception per sector

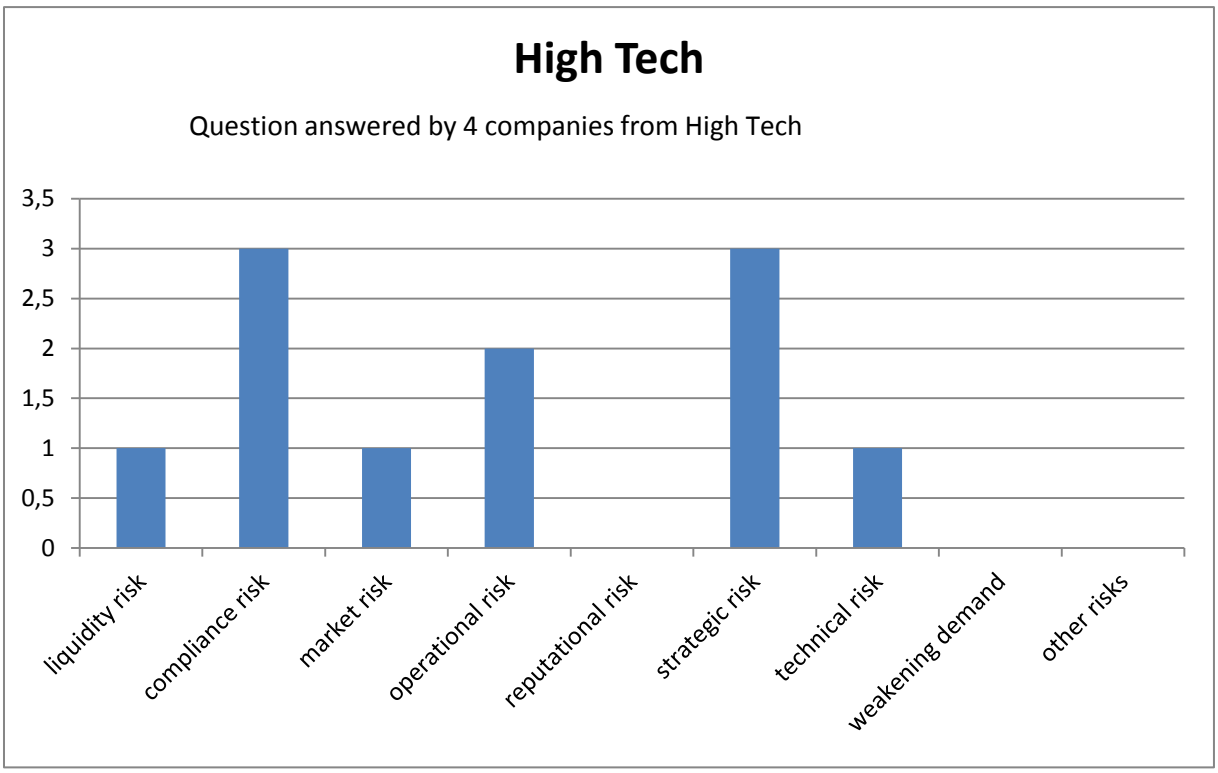


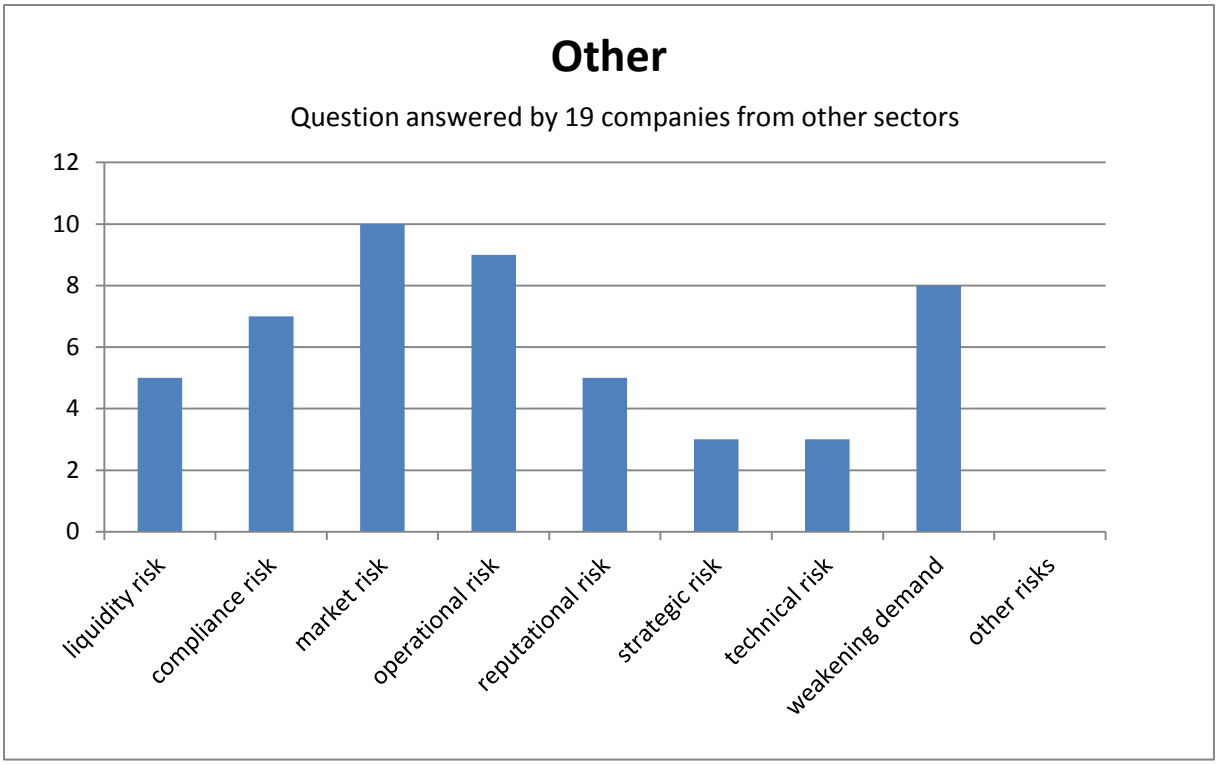



Retail
Question answered by 2 companies from Retail
2,5
2
1,5
1
0,5
0
liquidity risk
compliance risk
market risk
operational risk
reputational risk
strategic risk
technical risk
weakening demand
other risks


Healthcare
Question answered by 3 companies from Healthcare
2,5
2
1,5
1
0,5
0
liquidity risk
compliance risk
market risk
operational risk
reputational risk
strategic risk
technical risk
weakening demand
other risks


Public & Social Profit
Question answered by 3 companies from Public & Social Profit
2,5
2
1,5
1
0,5
0
liquidity risk
compliance risk
market risk
operational risk
reputational risk
strategic risk
technical risk
weakening demand
other risks


High Tech
Question answered by 4 companies from High Tech
3,5
3
2,5
2
1,5
1
0,5
0
liquidity risk
compliance risk
market risk
operational risk
reputational risk
strategic risk
technical risk
weakening demand
other risks


Other
Question answered by 19 companies from other sectors
12
10
8
6
4
2
0
liquidity risk
compliance risk
market risk
operational risk
reputational risk
strategic risk
technical risk
weakening demand
other risks