

# **RISK OVERSIGHT AT EXECUTIVE AND BOARD LEVEL**

Aantal woorden/ Word count: 24 952

**Annabelle Holvoet**

Stamnummer/ student number : 01313131

Promotor/ Supervisor: Prof. dr. ir. Regine Slagmulder

Masterproef voorgedragen tot het bekomen van de graad van:  
Master's Dissertation submitted to obtain the degree of:

Master of Science in Business Economics

Academiejaar/ Academic year: 2016 - 2017



# **RISK OVERSIGHT AT EXECUTIVE AND BOARD LEVEL**

Aantal woorden/ Word count: 24 952

**Annabelle Holvoet**

Stamnummer/ student number : 01313131

Promotor/ Supervisor: Prof. dr. ir. Regine Slagmulder

Masterproef voorgedragen tot het bekomen van de graad van:  
Master's Dissertation submitted to obtain the degree of:

Master of Science in Business Economics

Academiejaar/ Academic year: 2016 - 2017





## **PERMISSION**

I declare that the content of this Master's Dissertation may be consulted and/or reproduced, provided that the source is referenced.

Signature

Annabelle Holvoet

# ACKNOWLEDGEMENTS

This master dissertation is the conclusion of my master programme Business Economics at the University of Ghent. I challenged myself by choosing an unfamiliar topic. When I look back now, it has been an extremely educational experience. I met a lot of interesting people and companies during my case study, who all emphasised that risk management is a topical issue these days. I would like to express my personal gratitude to the people who supported me during this process.

First of all, I would like to thank my supervisor, prof. dr. ir. Regine Slagmulder, for her guidance and support over the last year. I really appreciate her valuable and regular feedback during the literature study and empirical research of this master dissertation.

I would also like to thank all the involved companies for giving me the opportunity to conduct interviews and for contributing to my empirical research. I spent a lot of time and effort on contacting the right person in each of the interviewed organisations. Nevertheless, I must admit that I was positively surprised by the great willingness of many companies to participate in my research.

I also want to give a special recognition to Mrs. De Wilde and her colleagues of BELRIM for contacting their members in the context of my case study. Moreover, I would like to thank her for inviting me at the event of BELRIM and the NBN concerning risk management standards. This gave me the opportunity to establish my first contacts with risk managers of Belgian corporations.

Finally, I would like to thank my parents and friends for always believing in me and supporting me during my academic career at the University of Ghent.

## TABLE OF CONTENT

Used abbreviations .....	V
List of figures .....	VI
List of tables .....	VI
Abstract in English .....	VII
Abstract in Dutch .....	VIII
1. Introduction .....	1
2. Risk management.....	2
2.1. Definition of risk management.....	2
2.2. Increased attention to risk management .....	2
2.3. Enterprise risk management.....	3
2.3.1. Definition of ERM .....	3
2.3.2. The rise and added value of ERM .....	4
2.3.3. Strategic risk management .....	4
2.4. Risk management structure .....	5
2.4.1. Chief risk officer or head of risk management.....	5
2.4.2. Risk committee at board level.....	5
2.4.3. Other risk roles .....	6
3. Corporate risk oversight.....	7
3.1. Executive management .....	8
3.1.1. General role of the executive management .....	8
3.1.2. The role of the executive management in risk management .....	8
3.1.3. Chief risk officer .....	8
3.1.4. Risk committee at executive level .....	9
3.2. The board of directors .....	10
3.2.1. General role of the board of directors .....	10
3.2.2. The role of the board of directors in risk management.....	10
3.2.3. Risk committee in the board .....	11
3.3. Internal risk reporting.....	13
3.3.1. Risk reporting content .....	13
3.3.2. Presentation of risks to the board .....	15
3.3.3. Frequency and timing .....	16
3.4. Determinants and consequences of risk oversight .....	17
3.4.1. Determinants of risk oversight .....	17
3.4.2. Consequences of risk oversight.....	19

4. Empirical study.....	20
4.1. Aim of the study .....	20
4.2. Research questions.....	20
4.2.1. Risk oversight structure and responsibilities.....	20
4.2.2. Strategic risk management.....	21
4.2.3. Internal risk reporting and information provision .....	21
4.2.4. Determinants.....	21
4.2.5. Consequences of risk oversight .....	21
4.3. Research methodology .....	22
4.3.1. Research design.....	22
4.3.2. Target group.....	23
4.3.3. Sample selection .....	23
4.3.4. Interview approach.....	25
5. Analysis.....	26
5.1. Methodology.....	26
5.2. Within case analysis.....	26
5.2.1. Colruyt.....	27
5.2.2. Proximus.....	30
5.2.3. Raffinerie Tirlemontoise.....	33
5.2.4. Ardo .....	35
5.2.5. Company A .....	37
5.2.6. Company B .....	40
5.2.7. Company C .....	43
5.2.8. Company D .....	45
5.3. Cross case analysis.....	48
5.3.1. Risk oversight structure and responsibilities.....	48
5.3.2. Strategic risk management.....	50
5.3.3. Internal risk reporting and information provision .....	50
5.3.4. Determinants.....	52
5.3.5. Consequences of risk oversight .....	57
6. Conclusion .....	58
6.1. General conclusions .....	58
6.2. Recommendations and limitations .....	60
REFERENCES .....	LXI
Appendix 1: Risk management process .....	LXVII
Appendix 2: The development of risk management .....	LXVIII



Appendix 3: Conceptual frameworks.....	LXX
Appendix 4: Strategic risk assessment process .....	LXXII
Appendix 5: Information processing.....	LXXIII
Appendix 6: Risk reporting structure .....	LXXIV
Appendix 7: Risk dashboard .....	LXXV
Appendix 8: List of companies in the target group.....	LXXVI
Appendix 9: Questionnaire – Dutch version .....	LXXVIII
Appendix 10: Questionnaire – English version.....	LXXX
Appendix 11: Company characteristics.....	LXXXII
Appendix 12: RQ1 and RQ2 - Risk oversight structure and SRM.....	LXXXIII
Appendix 13: RQ3 - Internal risk reporting and provision of information .....	LXXXV
Appendix 14: RQ4 - Determinants .....	LXXXVI
Appendix 15: RQ4 – Summary table.....	LXXXVIII
Appendix 16: RQ5 - Consequences of risk oversight .....	LXXXIX

## Used abbreviations

AC	Audit Committee
A&CC	Audit & Compliance Committee
BELRIM	Belgian Risk Management Association
BoD	Board of Directors
BU	Business Unit
CCAO	Chief Corporate Affairs Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organizations
CRMO	Chief Risk Management Officer
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
ExCo	Executive Committee
FERMA	Federation of European Risk Management Associations
GDPR	General Data Protection Regulation
HR	Human Resources
ICGN	International Corporate Governance Network
ISO	International Organization for Standardization
KPI	Key Performance Indicators
KRI	Key Risk Indicators
NACD	National Association of Corporate Directors
NBN	Bureau for Standardisation
NYSE	New York Stock Exchange
PR	Public Relations
RBV	Resource-Based View
RM	Risk Management
SRM	Strategic Risk Management

## List of figures

Figure 1: Classical risk map.....	15
Figure 2: Determinants and consequences of risk oversight .....	17

## List of tables

Table 1: List of Companies .....	24
----------------------------------	----

## Abstract in English

The increase in environmental complexity and the stricter corporate governance regulations have led to a growing external pressure for better risk oversight. This concerns the allocation of risk responsibilities at executive and board level, as well as their mutual collaboration and communication. The case study in this master dissertation makes use of in-depth interviews with eight different Belgian companies to examine how they are organised for effective risk oversight. First of all, I found that the majority of the interrogated organisations have a similar structure in place with a separate risk management department overseeing the risk process. They report at least quarterly towards the executive committee and the board. The final responsibility for risk management usually lies with an existing management position as none of the companies appointed a CRO nor board level risk committee. This can mostly be explained by the already high level of support from the top for risk management. Secondly, most companies are already aware of the benefits of strategic risk management, which is the link between risk management and the business strategy. However, there is still room for improvement in terms of a developed approach. Furthermore, I compared the different cases to define the determining variables of risk oversight. Especially firm size in combination with the ownership type, the degree of regulation and the level of support from the top were found to have a significant impact. Finally, attention was paid to the consequences of all these efforts for the company. In this respect, I especially noticed an influence on the corporate risk culture as there is a growing internal awareness for risk management.

## Abstract in Dutch

De toenemende complexiteit in de bedrijfsomgeving en de steeds strikter wordende regelgevingen omtrent corporate governance hebben geleid tot een sterk stijgende externe druk voor meer betrokkenheid van het uitvoerend management en de raad van bestuur op vlak van het risicobeheer van hun organisatie. Dit omvat de toewijzing van de verantwoordelijkheden, alsook de onderlinge samenwerking en communicatie tussen beide niveaus. De casestudy in deze masterproef is gebaseerd op diepgaande gesprekken met acht verschillende risicomangers van Belgische bedrijven. Ten eerste, vond ik dat de meerderheid van de ondervraagde bedrijven een gelijkaardige structuur hebben opgezet. Een onafhankelijke risico afdeling overziet het volledige proces en rapporteert ten minste elk kwartaal aan het directiecomité en de raad van bestuur. De eindverantwoordelijkheid voor risicobeheer ligt meestal bij een bestaande managementfunctie. De bedrijven hebben geen afzonderlijke CRO of apart risicocomité aangesteld aangezien er al voldoende ondersteuning komt van bovenaf. Ten tweede, zijn de meeste bedrijven al op de hoogte van de voordelen van strategisch risicobeheer of de link tussen risicobeheer en de bedrijfsstrategie. Anderzijds is er wel nog veel ruimte voor verbetering op vlak van een uitgewerkte aanpak. Verder vergeleek ik de verschillende bedrijven onderling om na te gaan welke variabelen een bepalende invloed hebben op risicobeheer. Hierbij vond ik dat vooral de bedrijfsgrootte in combinatie met het eigenaarschap een impact hebben, alsook het niveau van regelgeving en de steun van bovenaf. Tot slot onderzocht ik welke gevolgen dit nu heeft voor het bedrijf. Ik stelde hierbij hoofdzakelijk een impact vast op vlak van de risicocultuur van de organisatie, namelijk een toenemende interne belangstelling voor risicobeheer.

## 1. Introduction

Today's organisations are operating in a highly complex and rapidly changing environment caused by globalisation, technological advancements and many other worldwide events. This has led to an increase in the number and complexity of the risks facing the companies. In order to be aware of the threats and to be better prepared for the future, organisations have to establish effective risk management (Lam&Kawamoto, 1997; Raber, 2003; Berg&Westgaard, 2012; OECD, 2014). Over the past two decades, risk management has evolved towards a more enterprise-wide approach. Companies currently pay more attention to the interrelatedness between different risks. Moreover, there has been a shift in attention towards strategic risks and uncertainties (Frigo&Anderson, 2011; Berg&Westgaard, 2012).

Furthermore, there has been a significant increase in external pressure for enhanced risk oversight by the executive management and the board of directors. These calls especially ask for more board engagement in risk management. As the directors are held responsible for the overall business performance, they have to be aware of the key risks and include them in their discussions in the context of the business strategy. The board has in its turn placed greater expectations on the role of the executive team in the risk process (Atkinson, 2008; Van der Elst, 2013).

This master dissertation starts with a comprehensive literature study. First of all, the concept of risk management is described. Secondly, more information is provided on enterprise risk management. Subsequently, the focus is placed on the delegation of the risk roles and responsibilities to the executive and board level. This master dissertation also discusses how and when the executive and board level are provided with risk information. To conclude the literature study, I discuss some possible determinants and consequences of risk oversight. The second part of this master dissertation contains the empirical research, based on a case study of eight different Belgian companies. Five different research questions are being answered by means of a comprehensive analysis of in-depth interviews and corporate information. The final part of this paper describes the general conclusions and the recommendations for further research.

## 2. Risk management

### 2.1. Definition of risk management

Risk management can be defined as *“the holistic process involved in recognising possible risks, and the measures undertaken to reduce and monitor them”* (Kalia&Müller, 2007, p.23) or as *“a process by which the organisation assesses its exposure to types of harm, evaluates their impact, develops management strategies, and implements actions that manage risk to the level desired by the board”* (Spencer&Hyman, 2012, p.6).

Risk management consists of a loop that is being repeated over and over again by organisations to deal with uncertainty in their environment. An overview of the risk management process can be found in appendix 1. The cycle starts with risk perception and risk identification. Organisations must continuously observe their environment to be aware of every signal of increased risk. The second step is to communicate and analyse the risks. Finally, risks have to be assessed and the organisation should take adequate strategical actions to mitigate its effects. These actions have to be continuously monitored and evaluated to guarantee their effectiveness (Kalia&Müller, 2007; Van der Elst, 2013; Spencer&Hyman, 2012).

### 2.2. Increased attention to risk management

The first concepts of risk management appeared in the first half of the 20<sup>th</sup> century. The developments up until now are described in appendix 2. Over the past decades, the contextual environment of companies has significantly changed, with a rise in both the volume and the complexity of risks (Berg&Westgaard, 2012; OECD, 2014). The financial crisis of 2007-2008, for example, has contributed to an increase in companies' interest in risk management. Today, every organisation is confronted with a lot of risks. Despite the often negative connotation, taking risks is also important to create added value for the company (Van der Elst, 2013; Spencer&Hyman, 2012; Olson&Dash Wu, 2015).

The growing importance of risk management also stems from the imposed regulatory frameworks. Directives and regulations from the European Commission include strict disclosure requirements for organisations concerning their principal risks and uncertainties (European Commission, 2016)<sup>1</sup>. Moreover, individual countries as well have introduced strict risk management legislations (Van der Elst, 2013). Furthermore, multiple stock exchanges, such as the NYSE, are increasingly putting pressure on organisations to install effective risk management systems. The rising pressure is mainly focused on

---

<sup>1</sup> Both Prospectus Directive 2010/73/EU and Commission Regulation 809/2004 of the European Commission aim to protect investors by imposing minimum disclosure requirements for companies that offer securities to the public in the EU (European Commission, 2016).

the need for increased risk oversight by the executive and board level. The Securities and Exchange Commission (SEC), an agency of the U.S. federal government, also requires organisations to disclose comprehensive information on the risk management role of the board (Ballou, Heitger, &Stoel, 2011). Audit committees as well are having increased concerns regarding risk management. Their worries are related to the velocity of risks and the association between risk management and the business strategy (Kalia&Müller, 2007; Ballou et al., 2011; KPMG, 2010; Beasley, Branson, &Hancock, 2014). Finally, banks are attaching growing importance to ratings provided by credit rating agencies when assessing the organisation. These rating agencies also take the current state of risk overzicht into account when determining a company's rating. Therefore, the instalment of an effective risk management process provides the organisation with an improved rating and as a result, they have easier access to capital (Kalia&Müller, 2007; Frigo&Anderson, 2011; Beasley et al., 2014).

Despite the growing interest in risk management, there is still a large scoop for improving the current practices. Only one quarter of the organisations in a U.S. survey stated that they have formal and structured processes in place for risk management (Beasley, Branson, &Hancock, 2016).

## **2.3. Enterprise risk management**

### **2.3.1. Definition of ERM**

*“ERM seeks to strategically consider the interactive effects of various risk events with the goal of balancing an enterprise's portfolio of risks to be within the stakeholders' appetite for risk”* (Frigo&Anderson, 2011, p. 82). COSO<sup>2</sup> also provided a definition of ERM: *“ERM is a process, effected by the 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 the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”* (COSO, 2009, p. 2).

Traditional risk management includes the consideration of each risk on its own, without paying attention to the interactions between various risks. Different BUs within a company independently manage separate categories of risks without any mutual collaboration. Accordingly, traditional risk management is referred to as a 'silo' or 'stovepipe' approach. Many companies still apply this traditional model (Ittner&Oyon, 2014; Aksel, 2015). Enterprise risk management (ERM), by contrast, is a more advanced and enterprise-wide version of risk management as it reflects on the interaction between various risk classes. It requires more collaboration between the different corporate functions

---

<sup>2</sup> The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a cooperative union of five private organisations in the U.S. dedicated to assist companies in corporate governance by providing frameworks and general guidelines (COSO, 2009).



in order to oversee the portfolio of risks. ERM is a top-down approach, which means that the process starts at the top of the organisation, looking at the overall picture. Afterwards, focus is placed on the lower organisational levels for an effective implementation of ERM. The management of risks through an integrated, more holistic approach, creates more benefits for the company. Both definitions also mention that ERM attempts to balance an organisation's portfolio of risks with its stakeholders' risk appetite. This means that the company has to take account of the tolerable risk level of its stakeholders (Frigo&Anderson, 2011; Liebenberg&Hoyt, 2003; Ittner&Oyon, 2014). Different frameworks were developed to assist organisations in ERM. They describe the key principles of ERM and include guidelines for an effective implementation. Additional information on these frameworks and some prominent examples are described in appendix 3.

### **2.3.2. The rise and added value of ERM**

The broader dimension of risks, increased external pressure for corporate governance and recent technological developments all contributed to more holistic risk management. First of all, globalisation, the increased consolidation of sectors and the heightened regulation have led to an increase in the volume and complexity of risks (Law&Kawamoto, 1997). Secondly, regulatory instances have tightened the corporate governance regulations (Law&Kawamoto, 1997). They also obliged organisations to have a more company-wide overview of their risks. Finally, recent developments in information processing technologies enabled companies to quantify risks and improve their risk analysis process (Liebenberg&Hoyt, 2003). Moreover, these new techniques assist managers in understanding the interdependencies between various risk classes (Miller, 1992; Jablonowski, 2001).

Initially, organisations implemented ERM to comply with the corporate governance requirements. However, nowadays, organisations increasingly realise that it is in their own interest to implement ERM as it creates added value for the company (Beasley&Frigo, 2007). First of all, ERM ensures the availability of more and better information on the company-wide risk profile, which leads to better decision-making (Kalia&Müller, 2007; Frigo&Anderson, 2011; Aksel, 2015). Secondly, by managing risks in an integrated way, the entire organisation is involved which creates synergies between the different departments and avoids duplication of expenses (Miccolis&Shah, 2000; Aksel, 2015).

### **2.3.3. Strategic risk management**

When comparing the two definitions of ERM at the beginning of this section, it is clear that they both include a link between risk management and the business strategy. Strategic risk management (SRM) can be defined as *“a process for identifying, assessing and managing risk anywhere in the strategy with the ultimate goal of protecting and creating shareholder value”* (Frigo&Anderson, 2011, p. 84). The main idea of SRM is that organisations need to better align their risk management and risk appetite

with the strategic decision-making process. SRM includes identifying the critical risks inherent to the corporate strategy, a process which is often referred to as strategic risk assessment. Strategic risks are those risks that are closely related to the overall business strategy. They can have a large influence on the predetermined objectives and therefore deserve a significant amount of time and attention from the executive and board level (Frigo&Anderson, 2009). Incorporating ERM in the strategy crafting process creates additional value for the organisation and its stakeholders (Frigo&Anderson, 2009; Beasley et al., 2016). Appendix 4 contains an overview of the strategic risk assessment process.

## **2.4. Risk management structure**

In order to establish effective risk management, the concerning responsibilities have to be distributed among the different organisational levels and positions. The risk management structure should set the tone for the right ERM culture (Aksel, 2015). Next to the already existing positions of CEO, executive committee and board of directors, several other positions can be created to improve the functioning of risk management. Examples of possible functions are described in the following sections.

### **2.4.1. Chief risk officer or head of risk management**

An increasing number of companies opts to allocate the final responsibility for risk management to a single individual in the executive committee. This person is then called the CRO or the head of risk management. More information on this important position can be found further in this paper (3.1.3. *Chief risk officer*).

### **2.4.2. Risk committee at board level**

Traditionally, organisations mainly dealt with risks and their consequences at the operational and management level. However, in order to achieve effective results, risks should also be monitored at board level (Hilb, 2012). Stricter corporate governance regulations have also led to an increase in the board's attention to risk management (Law&Kawamoto, 1997). While the board as a whole has a general overview on risk management, more specific responsibilities are usually assigned to separate board committees. These often include the board level finance and audit committees. Driven by the emergence of ERM, organisations began to realise that these existing committees are already overwhelmed with multiple tasks, so they started to create separate risk committees at board level (Atkinson, 2008). More information on risk committees can be found further in this paper (3.2.3. *Risk committee in the board*).

### 2.4.3. Other risk roles

Companies are usually composed of different BUs or departments. They can appoint a **risk coordinator** at every unit, who then has to carry out the same responsibilities as the head of risk management, but at a lower organisational level (Kalia&Müller, 2007). Sometimes a certain risk can be so important that a **risk owner** is appointed. This individual is then held responsible for managing this specific risk. Besides reflecting on the necessary mitigating actions, the risk owner has to report the risk status to the higher corporate levels. Similarly, one or more individuals can be held responsible for the implementation of the mitigating actions. These people are called **response owners** and they also have to report on their actions to the executive management (Kalia&Müller, 2007; Ittner&Oyon, 2014).

Furthermore, organisations can choose to designate **risk champions** for more effective risk management. These company members must ascertain that risk management is part of the corporate culture. As opposed to the abovementioned functions, risk champions do not have to be part of the risk management team and they do not have to be experts in risk. By way of contrast, they are expected to have a very good knowledge of the organisation and its culture. They have to be able to involve other people through their excellent social skills and effective communication. Risk champions have to convince other company members to be attentive for risks in their daily activities. Besides risk champions who are not part of the risk management team, the CRO and the risk coordinators are also considered to be risk champions (Kalia&Müller, 2007).

Traditionally, risk management especially and almost only encompassed financial and insurance risks. Over the past decades, different global events increased the necessity of a wider approach on risk management. Nevertheless, some organisations still hold their **CFO** responsible for risk management because of his expertise in finance and insurance (Ittner&Oyon, 2014).

Additionally, the **internal audit department** also takes on risk responsibilities such as evaluating the most important risks, assessing ERM processes and reporting on their diligence to the board. Multiple companies also delegate risk oversight responsibilities to the audit committee (Spira&Page, 2003; Kalia&Müller, 2007; Protiviti, 2010; Tonello, 2012; Ittner&Oyon, 2014).

### 3. Corporate risk oversight

Risk management still has to deal with a lot of weaknesses (Hilb, 2012). One of the major issues is the fact that the many companies particularly deal with risks at their operational and managerial level, while there is little involvement of their board level. As mentioned before, recent more stringent regulations on corporate governance call for a greater involvement of boards in risk management. This is referred to as risk oversight (Protiviti, 2010; Ballou et al., 2011; Tonello, 2012; Van der Elst, 2013; Ittner&Keusch, 2014; Gupta&Leech, 2014). Risk oversight is defined as: *“the board’s supervision of the risk management framework and risk management process”* (ICGN, 2015, p.5). Corporate risk oversight enables the executive management and the board to have a proper understanding of the company’s critical risks and associated actions, as well as its general risk profile. It also includes the mutual communication and ongoing reporting concerning the risk approach between the executive and board level (Tonello, 2012; COSO, 2013; Ittner&Keusch, 2014). Risk oversight is different from risk management, which is the more practical implementation of the risk approach by the lower organisational levels (ICGN, 2015).

Previous research found that explicitly defining the board’s responsibilities regarding risk management leads to more mature ERM practices in the company (Ittner&Keusch, 2014). COSO issued its *“Effective Enterprise Risk Oversight: The Role of the Board of Directors and Strengthening ERM for Strategic Advantage”* to assist companies in risk oversight. First of all, the executive management and the board should have a shared view on the risk appetite and risk culture. The risk appetite is the level of risk that is acceptable within the company. Secondly, the board should have a proper understanding of how the executive management is addressing the risks. Next, the COSO paper advises companies to use a portfolio perspective on risks to see the interrelationships. Finally, the board has to be aware of the key risks facing the firm and the associated mitigating actions (COSO, 2009; Protiviti, 2010; Ballou et al., 2011; Gupta&Leech, 2014).

This chapter provides information on the different organisational positions at executive and board level in the area of risk oversight. The actual structure can vary from a centralised model with only one person held accountable for risk oversight, to a model where the responsibility has been distributed across different organisational levels and functions. On the one hand, a centralised model has the advantage of providing a more coordinated and integrated approach. Moreover, the person who is held accountable for risk oversight will have a profound understanding of the overall risk portfolio of the firm and the relationships between different risks. On the other hand, companies that opt to spread the accountability across different organisational parts, will benefit from the variety of knowledge and expertise of different people (Ittner&Oyon, 2014).

### **3.1. Executive management**

#### **3.1.1. General role of the executive management**

The executive management is a team of professionals who are responsible for the daily management of the company. They are the leaders of the diverse organisational departments. In order to achieve the company's objectives, they have to make operational decisions and they must deploy the resources in the best interest of the organisation. Moreover, they are held responsible to keep the board up to date by regularly providing them with information on all organisational aspects (Mintzberg, 1989).

#### **3.1.2. The role of the executive management in risk management**

The executive management is held responsible for the assessment, planning and implementation of risk management, assisted by the organisational staff. In particular, the management team draws up proposals for the establishment of effective risk systems. These then need to be approved by the board. Afterwards, the executive management's main priority is to enact the agreed risk direction (Spencer&Hyman, 2012). Both new regulations and stricter requirements concerning corporate governance call for a better definition of the risk roles of senior executives. As a consequence, several organisations have appointed a CRO in their executive committee (Law&Kawamoto, 1997).

#### **3.1.3. Chief risk officer**

The title of CRO has only recently been added to the collection of corporate positions. The institution of the first CRO dates back to 1993, when James Lam was the first to get this formal title at GE Capital (Kalia&Müller, 2007). At first, especially U.S. financial services organisations appointed a CRO. The external pressure for better risk oversight and the recognition of the added value of ERM have both contributed to a growing number of organisations, active in other industries and other geographical regions, dedicating a specific management position to risk management (Lam, 2001). ERM lead, chief risk management officer (CRMO) and enterprise-wide risk manager are synonyms for the same title (Branson, 2015; Aksel, 2015).

A CRO has the ultimate responsibility for the implementation of a company-wide risk programme that has to be in accordance with the risk appetite (Lam&Kawamoto, 1997). His main priority is the integration and coordination of all aspects of risk management. Moreover, a CRO serves as a risk champion within the organisation as he has to promote ERM and create a high level of risk awareness amongst the organisational members (Liebenberg&Hoyt, 2003). A CRO is also considered to be the management liaison to the board as he has to provide the board members with risk information (Lam, 2001; Kalia&Müller, 2007; Ittner&Oyon, 2014; Aksel, 2015).

Sometimes, organisations designate multiple CROs, with each BU having its own CRO and a corporate CRO who oversees the whole risk process (Boyd, Moolman, & Nwosu, 2016). The appointment of a CRO in the organisation mostly has a positive association with the maturity level of ERM (Beasley et al., 2016). Creating a CRO position stresses both internally and externally the company's commitment to ERM (Lam, 2001; Liebenberg & Hoyt, 2003).

The required capabilities to become a CRO depend on the size and characteristics of the organisation, as well as on the industry. The necessary skills, knowledge and experience are rarely found in one individual. Risk managers are often experienced in market risk, credit risk or operational risk, but only seldom they are expert in all risk categories (Liebenberg & Hoyt, 2003; Aksel, 2015). A good CRO mostly has a high educational degree and is technically very solid (Thiessen, Hoyt, & Merkley, 2001). Since the CRO has to communicate frequently with the CEO and board members, excellent communication and coordination skills are indispensable (Lam, 2001; Liebenberg & Hoyt, 2003).

#### **3.1.4. Risk committee at executive level**

Proponents of ERM believe that a corporate risk programme needs someone who carries the final responsibility for the internal risk coordination and communication (Liebenberg & Hoyt, 2003). Despite the agreement on the importance of a responsible body, there is disagreement on its structure. Some argue that the programme should be overseen by a single person such as a CRO, others favour a risk committee at executive level (Haubenstock, 1999). Especially in larger and more complex organisations, executive level risk committees are being appointed as a management partner for the board level risk committee. While the board risk committee is responsible for risk oversight, the executive risk committee is in charge of the actual implementation of the risk programme (Bugalla, Kallman, Mandel, & Narvaez, 2012). The majority of organisations believe that a CRO and an executive risk committee can complement each other (Miccolis & Shah, 2000).

The formation of an executive risk committee guarantees that the risk management responsibilities are spread across multiple executives with different capabilities and backgrounds. It is often composed of the most important executive managers of the company. This in its turn promotes a more holistic and comprehensive view on risk management and a better understanding of the interrelationships between different risks (Bugalla et al., 2012). Organisations with interdisciplinary risk committees at management level tend to have a more cross-functional approach towards risk management (Bugalla et al., 2012; Ittner & Oyon, 2014).

## 3.2. The board of directors

### 3.2.1. General role of the board of directors

The board of directors consists of both executive and non-executive members that have been elected by the shareholders. Their key role is to supervise the company for the benefit of both internal and external stakeholders. On the one hand, internal stakeholders should receive guidance and supervision, as well as relevant information from their corporate board. On the other hand, the board is held accountable for the information provision towards the external stakeholders regarding the company's operations and results (Van der Elst, 2013). Furthermore, board members have to approve the long-term business strategy and develop an adequate resource allocation. They also have to appoint and remunerate the CEO and his management team. Finally, directors have the decision-making authority to develop the corporate policies and define the organisational objectives (Tricker, 1994; Ingley&Van Der Walt, 2008).

Over time, different theories have been developed regarding the role of the board. The **agency theory** describes solutions for problems in the relationship between two parties, the principal and his agent. This theory suggests that there are conflicts of interests between the owners of the company and the management level. It therefore emphasises the controlling and monitoring role of the board. The **stewardship theory**, meanwhile, focuses on the strategic role of the board. This theory suggests that managers are inherently operating in the interest of the company, so there is no need for the board to control their activities. As a consequence, the role of the board is restricted to reviewing and approving the strategy proposal drawn up by the management team. The **stakeholder theory** advocates the coordinating role of the board. It states that the board is responsible for the communication and negotiation between the company and its internal and external stakeholders (Hung, 1998).

### 3.2.2. The role of the board of directors in risk management

#### *Monitoring role*

The ultimate responsibility for risk oversight lies with the entire board of directors (Tonello, 2012). They are accountable to the organisational stakeholders (Dickinson, 2001). The role of the board in terms of risk management is similar to their overall responsibility for the strategy and processes. The board has to provide general guidance and supervise the risk management process and practices (Raber, 2003; Ittner&Keusch, 2014). First of all, board members have to approve the company-wide risk approach and the accompanying risk policies and procedures proposed by the executive level. These must be synchronised with the predetermined risk appetite (Kalia&Müller, 2007; Spencer&Hyman, 2012). Secondly, the board has to supervise the risk implementation process to make sure that the management team carries out its tasks in a proper way (Ernst&Young, 2013; ICGN, 2015).

A risk process is only beneficial if everyone in the organisation is convinced of its benefits and if people are willing to be involved. Risk management has to be part of the organisational culture and should be reflected in the values of the company (Spencer&Hyman, 2012). Together with the risk champions, the board is responsible to establish a supportive culture that encourages openness and internal dialogue on risk and strategy. They should repeatedly communicate the importance of risk management and provide supporting guidelines. In summary, the tone of risk management has to be set at the top of the organisation to reach the bottom of the firm (Kalia&Müller, 2007; Brodeur, Buehler, Patsalos-Fox, &Pergler, 2010; ICGN, 2015).

#### *Strategic risk management by the board of directors*

As mentioned before, linking risk management with the corporate strategy is of major importance for organisations operating in a today's complex and rapidly changing environment. Strategy and risk management have become inseparable (ICGN, 2015). It therefore comes as no surprise that SRM is considered to be a core competence of the board. Boards have to make sure that risks are incorporated in the strategy process: *"Risk is an integral part of every company's strategy; when boards review strategy, they have to be forceful in asking the CEO what risks are inherent in the strategy"* (Charan, 2009, p.23). Boards should consult their management team to gain information on the risks inherent to the business strategy and to include these risks in the strategy process. Key risk indicators (KRIs) are metrics that provide a signal when a certain risk is significantly increasing. These indicators can be developed in order to facilitate the monitoring task of the board and they assist organisations in determining the effectiveness of mitigating actions (Fraser&Simkins, 2009; Zhang, 2010).

#### **3.2.3. Risk committee in the board**

Instead of only holding the board as a whole responsible for risk management, some companies delegate risk responsibilities to one or more specific board committees. The main purpose of a company-wide risk committee is to assist the board in overseeing the ERM process (Bugalla et al., 2012). It has to monitor all the different risks from an overall company basis, as well as the associated actions (Lam&Kawamoto, 1997; Atkinson, 2008). Companies face a very broad range of risks, encompassing different organisational functions. Therefore, risk committees must be composed of people with different backgrounds and expertise (Lam&Kawamoto, 1997). Members of a risk committee are often chairs of other board level committees. As a result, they have a profound understanding of the organisational operations, strategy and the different risks facing the company. In order to be effective, the committee should also engage independent directors who have experience within the industry. The committee should not only comprise risk management professionals, but also experts on audit, compliance, HR and PR. These professionals must support the different BUs by providing effective approaches and tools for risk management (Lam&Kawamoto, 1997; Atkinson, 2008;



Tonello, 2012; ICGN, 2015). Some organisations install separate committees, such as a technology committee or health committee, that are then responsible for a specific risk area without giving them the explicit name of a 'risk committee' (Tonello, 2012).

The responsibility for risk management at board level was traditionally shifted to the audit and finance committees (Bugalla et al., 2012). These committees, however, usually have a lot of other duties and responsibilities. Together with the increasing interest in ERM, organisations became aware of the need for a stand-alone risk committee at board level (Atkinson, 2008). Only this makes it possible to take the burden away from other committees. Moreover, audit committees do not always have the right skills to manage business or operational risks since their members usually have a more financial background (Tonello, 2012).

Establishing a separate risk committee offers the benefits of a greater focus on and increased attention to risk management, as well as more independent judgement (Tonello, 2012; Ittner&Keusch, 2014; ICGN, 2015). Prior studies found that the involvement of the board in risk management is stronger when roles have been explicitly designated. Nevertheless, the involvement level is lower for companies that only delegate the responsibilities to one or more board committees than for those companies that allocate the responsibilities to the board as a whole or to both the entire board and a separate board committee. After all, risk oversight remains a responsibility of the entire board. So when an organisation creates a separate risk committee, the remainder of the board must be kept informed on the key risks and their evolution (Brodeur et al., 2010; Tonello, 2012; Ittner&Keusch, 2014).

### 3.3. Internal risk reporting

Boards should receive timely, relevant and reliable information about risks facing the company and the associated mitigating actions to effectively carry out their risk oversight role. There should be an ongoing communication between the executive and board level (Bugalla et al., 2012). OECD principles<sup>3</sup> mention that the board should disclose risk information to the organisational environment and stakeholders (OECD, 2014). In order to do so, the board has to stay up-to-date and supervise risk management (Berg&Westgaard, 2012). Reporting is often mentioned as an important practice to control the organisation (Kurland, 1994; Ingley&Van Der Walt, 2008; Branson, 2015; DeLoach, 2016). In addition, reporting risk information to the board can help to assess whether the risk appetite of the executive and board level are aligned. (Denis, 2001). The next paragraphs investigate different characteristics of internal risk reporting, such as the content, the manner of presentation, the frequency and the timing.

#### 3.3.1. Risk reporting content

Communication between the executive and board level entails written reports, as well as oral presentations (Kurland, 1994). Especially large organisations and public companies provide their boards with written preparations monthly, quarterly or annually (Beasley et al., 2016). The information provided to the board particularly consists of financial and management accounts, but other important data such as risk information is also included (Johanson, 2008).

A typical risk report to the board covers the top risks facing the company. The current and previous status of every particular risk are included, as well as the frequency of occurrence and the KRIs (Kalia&Müller, 2007; Spencer&Hyman, 2012). The report often mentions the risk owners and their specific efforts to handle the risks. In order to provide the board with a clear view on the evolution of a risk and the effectiveness of the mitigating actions, a time-series analysis can be included. Furthermore, a risk report often contains a comparison between the effectiveness of the response actions and the predetermined KPIs (Kalia&Müller, 2007; Brodeur et al., 2010; Spencer&Hyman, 2012).

Once a year, the report may include an overview of the risk management quality. Quality control is usually carried out by the internal audit function and the head of risk management. Internal control especially focuses on the implementation of the mitigating actions, while the head of risk management compares risk management with other organisations and gives guidelines for continuous improvement. For Belgian organisations, BELRIM (Belgian Risk Management Association) brings risk

---

<sup>3</sup> OECD principles are non-binding standards of corporate governance, issued by the Organization for Economic Cooperation and Development (OECD, 2014).

managers of different companies and sectors together so that they can share their knowledge and experiences and learn from each other's best practices. The association arranges work groups, conferences and other activities in order to improve the quality of risk management in Belgium (Kalia&Müller, 2007; Protiviti, 2010; BELRIM, 2017).

When having a look at the number of risks reported to the board, this can vary strongly across organisations. While some boards only receive a limited number of three to five risks, others receive a comprehensive enumeration of ten to fifteen risks. In order to prevent the risk report of becoming too comprehensive and irrelevant, risk information should be analysed and prioritised. Therefore, risks are often ranked based on their probability of occurrence and their potential impact on the organisation (Kalia&Müller, 2007). Firms can divide the risks into tiers to make a differentiation between top-tier risks and lower-tier risks. The former risks can then be presented to the full board, while the latter risks only reach the audit or risk committee. Organisations might also prefer to sort the risks based on other criteria, such as their velocity or their financial impact (Branson, 2015).

In addition, managers can order the top risks into different categories. They often categorise risks based on the organisational structure. Some risks concern the organisation as a whole, while others are more of importance to a specific functional department. However, allocating a risk into a single category may cause more disadvantages than it provides benefit for the firm since it does not match with the main principle of ERM to consider the interrelationships between risks (Branson, 2015). COSO's 2009 *ERM – Integrated Framework* also includes a guideline to structure risks. The framework mentions four categories: strategic risks, operational risks, financial risks and compliance risks (COSO, 2009; Branson, 2015). Boards mainly receive information regarding operational risks. Previous studies found that there is still room for improvement relating to the supply of information on strategic risks facing the company (Ballou et al., 2011). This is in accordance with the growing importance boards place on SRM.

The resource-based view (RBV) is a theory on corporate resources that promotes the idea of both focusing on the static and dynamic dimension of resources. When applying this on board information, it means that we should not only examine which data the board receives (static dimension), but also how the board processes this information (dynamic dimension) (Zhang, 2010). This is a very interesting insight, but as it goes beyond the scope of this paper, I have included this in appendix 5.

### 3.3.2. Presentation of risks to the board

In most companies, the board already receives written risk information before the actual presentation of the risks during the board meeting. This ensures that the board is up-to-date on the current status of the risks facing the company (Kurland, 1994; Branson, 2015). The actual presentation of the top risks to the board is a duty of top management and is mostly led by the CRO (Berg&Westgaard, 2012). Sometimes there might be an intermediate stage, where the CRO presents the risks to a board committee or CEO before the risks reach the entire board (Branson, 2015). However, different researchers mention that the effectiveness is higher when the CRO reports directly to the board (Lam, 2001; Beasley et al. 2016). Appendix 6 contains an example of an organisational structure for effective risk reporting to the higher corporate levels.

The actual risk presentation usually consists of a combination of information elements. First of all, it almost always contains a narrative discussion between managers and directors on the key risks facing the company. Besides that, managers generally also give an explanation of the ERM process. During this discussion, the mitigating activities are also clarified. Secondly, managers make use of visual elements to inform the board on the risks in a clear and structured way. There are various types of graphical representation techniques, with a risk map as the most commonly used one. Organisations can also use scorecards, dashboards, charts or graphs to present the risks to the board (Branson, 2015).

#### *Risk map*

In order to visually indicate the different top-tier risks, managers can make use of a heat map or risk map. Risk mapping is the process in which the organisation tries to identify, quantify and prioritise risks. Risks are being ranked based on their likelihood and impact, while paying attention to the business strategy (Kalia&Müller, 2007).



Figure 1: Classical risk map. Source: Kalia&Müller, 2007.

This process results in a map with four different quadrants that give an indication of the priority that should be given to each risk. The figure above is an example of a classical risk map. Risks in the upper right quadrant are typically known to have a big impact on the functioning of the organisation and a high probability. Therefore, these risks should be closely monitored. Conversely, risks in the bottom left corner of the map demand less attention as they are less likely to happen and their impact on the organisation is minimal. Other dimensions can be added to the map by using different colours and sizes of the risk bubbles. Examples of additional criteria are the velocity of a risk, management's assessment, the risk area etc. (Brodeur et al., 2010; Branson, 2015).

#### *Risk dashboard*

While a risk map only displays risks on two different axes, a risk dashboard contains more detailed information on every risk facing the company. It is a comprehensive figure that gives a clear definition of every risk, as well as information on its current status. This status can vary from high to medium or low risk, depending on the urgency to intervene, and is often indicated with a colour. Furthermore, the mitigating actions are described and each risk is also coupled to a specific risk owner. An example of a risk dashboard is provided in appendix 7 (Branson, 2015; Boyd et al., 2016).

#### **3.3.3. Frequency and timing**

More than 50% of the surveyed board members in a U.S. survey said that they receive at least annually a risk report from their management team. Approximately half of the respondents argued that they receive the reports more frequently, which means that they receive those reports semi-annually or quarterly. Next to the annual report to the full board, many organisations provide more frequently an additional report to the risk and/or audit committee. None of the surveyed companies are reporting more frequently than quarterly (Branson, 2015). Multiple studies revealed that the regularity of risk reporting to the board should be increased (Protiviti, 2010).

Next to the frequency, it is also important to carefully consider the timing of the risk reports. No evidence has been found for a fixed pattern in the scheduling of risk reporting. Sometimes the timing of risk reports in U.S. companies is linked to filing with the SEC, either prior to it or immediately afterwards. Other companies' risk reports to the board coincide with the scheduled discussions on the business strategy (Branson, 2015).

### 3.4. Determinants and consequences of risk oversight

The aim of this master dissertation is to examine risk oversight in Belgian companies. Previous studies repeatedly investigated how risk management is implemented in Belgian companies and how risk reporting to external stakeholders is organised. Despite the increase in external pressure for more managerial and board engagement in risk management, the number of studies on risk oversight at the executive and board level in Belgian companies is rather limited. By focusing at this topic, this master dissertation fills this research gap and further complements the already existing findings on risk management in Belgian companies. Nevertheless, previous findings about risk management in Belgian companies and prior studies on risk oversight practices in other countries can serve as a foundation for this investigation. They help to determine possible determinants and consequences of risk oversight in Belgian companies. Figure 2 below shows the theoretical framework adopted in this paper.

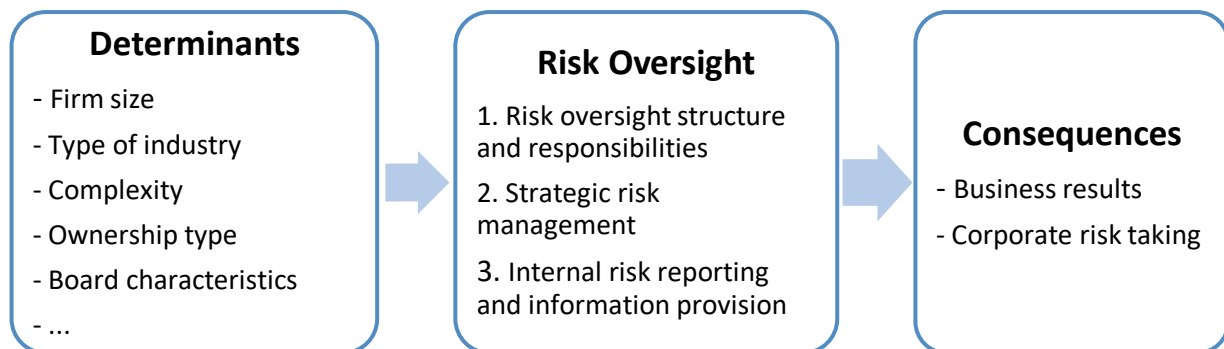


Figure 2: Determinants and consequences of risk oversight

#### 3.4.1. Determinants of risk oversight

##### *Firm size*

Prior studies found that larger organisations have more financial and human resources at their disposal to support their risk programmes. These companies need better risk management systems as they have to deal with more diverse and more complex risks compared to smaller organisations (Ellul&Yerramilli, 2013; Beasley et al., 2016). Therefore, large organisations are expected to have a more formal designation of the risk roles and responsibilities (Protiviti, 2010; Ittner&Oyon, 2014; Ittner&Keusch, 2014; Beasley et al., 2016). Regarding the assignment of accountability for risk oversight at executive level, larger organisations are more likely to appoint a CRO to oversee the risk management process. Moreover, they are often in favour of installing a separate managerial level risk committee. Large companies also tend to delegate the risk responsibilities to a board level committee or to both the board as a whole and a board level committee. Given the complexity of their risks, they opt to appoint a specific team of people instead of only requiring the board as a whole to oversee the risk process. In addition, they are more likely to install a separate risk committee at board level

compared to smaller firms. However, the majority still prefers to assign risk responsibilities to the audit committee rather than delegating them to a separate risk committee (Liebenberg&Hoyt, 2003; Atkinson, 2008; Tonello; 2012; Ittner&Keusch, 2014; Ittner&Oyon, 2014; Beasley et al. 2016). Previous findings also claim that larger companies usually have more advanced risk reporting practices to their executive and board level (Beasley et al., 2016). Overall, I expect firm size to be positively correlated with the maturity level of a company's risk oversight and risk reporting practices.

#### *Type of industry*

Previous studies often differentiated between financial and non-financial companies to investigate risk management (Ittner&Keusch, 2014; Beasley et al., 2016). However, as further explained, financial companies will not be included into the sample of this study. Nevertheless, there are other reasons to consider the type of industry as a determinant of risk oversight. First of all, the level of regulation in the industry will have an impact on the company's risk oversight since every sector is subject to other legislations. Because of this I expect to find significant differences between risk oversight practices across different industries. Prior studies found a positive link between the level of regulation in the industry and the instalment of a separate risk committee at board level. Secondly, different industries are subject to different risks, so this can also influence a company's risk approach (Atkinson, 2008; Ittner&Oyon, 2014).

#### *Complexity*

In terms of complexity as a possible determinant, I distinguish between the number of geographical regions in which the firm is operating and the number of business units in the organisation. First of all, organisations that are active in multiple geographical regions face more diversified risks. As a consequence, they attach more importance to risk management and I expect them to have more attention to risk oversight at the higher organisational levels. Secondly, the same conclusions can be drawn for organisations that are composed of different BUs and/or that are active in multiple different industries (Tonello, 2012; Ittner&Keusch, 2014).

#### *Ownership type*

The ownership type of the company is often mentioned as a determinant for its risk approach. One factor that can influence risk oversight is the distinction between publicly listed and privately held companies. Since publicly listed firms are in most cases also larger corporations, the same conclusions can be drawn as for the firm size. I expect publicly listed firms to attach more importance to the formal assignment of risk accountability. More specifically, they are more likely to assign the responsibility to a board level committee compared to privately held companies. In accordance with the findings for larger organisations, publicly listed firms are more likely to appoint a CRO and to install a managerial level risk committee. In terms of internal risk reporting, prior studies found that boards of public

companies receive more regular information on the key risks than the boards of private firms since they are, in turn, expected to provide risk information to the firm's external stakeholders (Protiviti, 2010; Ittner&Keusch; 2014; Beasley et al., 2016). Another possible determinant that has to be examined is the concentration of ownership, or more specifically, whether the shares belong to one powerful owner or the ownership is widespread over multiple different parties. Finally, risk management can also be influenced by whether the firm is a family business or not. Family businesses often look for stable long term results and therefore avoid serious risks and uncertainties. As a consequence, a strong risk management function is of major importance for them (McKinsey, 2010).

#### *Board characteristics*

Many researchers include different board characteristics into their set of variables when conducting research into risk management. They investigate the influence of the number of directors and the level of board independence. Results indicate that larger boards are more likely to assign the responsibilities to the board as a whole instead of to a separate board committee (Ittner&Keusch, 2014).

#### *Other determinants*

Besides investigating the influence of the abovementioned variables, this master dissertation also aims to identify other determinants of risk oversight in order to contribute to the existing knowledge.

### **3.4.2. Consequences of risk oversight**

Sceptics argued that risk oversight practices are often window-dressing in order to be compliant with certain regulations, rather than for the benefit of the company. Therefore, researchers studied the impact of risk oversight on the company's results and on corporate risk taking. First of all, they found that the maturity level of risk oversight practices shows a positive association with the general maturity level of risk management in the firm. This in its turn has a positive influence on the general results of the company (Ingley&Van der Walt, 2008; Ittner&Keusch, 2014). Another previous investigation has also demonstrated that strong risk management functions have multiple positive consequences for companies. These benefits include better operating results, higher stock return and a higher level of return on assets (Ellul&Yerramilli, 2013). Secondly, previous studies discovered an indirect association between the maturity level of a company's risk oversight and its risk behaviour. More specifically, they discovered that organisations with more advanced risk oversight systems are more likely to take risk-averse decisions (Ingley&Van der Walt, 2008; Ittner&Keusch, 2014). A better developed risk management function restrains those actions and decisions of managers and directors that favour excessive risk taking. A company's level of risk taking is usually measured by gathering data on the volatility in its stock returns (Ellul&Yerramilli, 2013). In conclusion, I expect risk oversight to have beneficial influences on the business results and the company's level of risk taking.



## 4. Empirical study

### 4.1. Aim of the study

The main purpose of this paper is to investigate how risk oversight is organised at the executive and board level of Belgian companies. As previously mentioned, I will thereby contribute to the existing knowledge on risk management in Belgian organisations. The study focuses on three specific areas of risk oversight. First of all, research is conducted on how the risk roles and responsibilities are delegated to different bodies and individuals at executive and board level. Secondly, research is conducted on SRM in Belgian companies. Finally, the study examines the internal risk reporting practices at the executive and board level of Belgian organisations. Overall, I expect to discover some general patterns and similarities across the organisations with respect to the three main research topics. Nevertheless, I also assume that companies will differ in their risk approach, since all the systems and structures need to be tailored to their unique characteristics, needs and circumstances. Furthermore, this master dissertation investigates whether particular organisational characteristics have an influence on a company's approach to risk oversight. Finally, the study aims to assess the impact of risk oversight on organisational results and risk behaviours.

### 4.2. Research questions

#### 4.2.1. Risk oversight structure and responsibilities

**Research Question 1:** *How are risk oversight roles assigned at executive and board level in Belgian corporations?*

The literature study highlighted the importance of explicitly assigning accountability for risk management at the executive and board level of an organisation. However, there is a lot of debate on the most effective organisational structure for risk oversight. Therefore, the first research question addresses this issue. More specifically, at managerial level, the study investigates whether the organisation has appointed a CRO and/or a managerial level risk committee. At board level, the study examines whether companies delegate risk responsibilities to the entire board or to a board committee. In case of a board committee, further research is conducted into the nature of this committee as it can either be a separate risk committee or an extension of the role of an already existing one such as the audit committee. The study not only examines who has been appointed, but also describes which responsibilities regarding risk management they have to fulfil.

#### 4.2.2. Strategic risk management

**Research Question 2:** *To what extent do Belgian companies link risk management with their business strategy process?*

The literature study revealed the increase in attention to SRM. The second research question investigates whether Belgian companies see ERM as a strategic tool. More specifically, I will investigate whether and how their boards incorporate top risks facing the company in their strategy process.

#### 4.2.3. Internal risk reporting and information provision

**Research Question 3:** *How is internal risk reporting and information provision organised in Belgian corporations?*

Besides stressing the benefits of an appropriate risk oversight structure, the literature study pointed at the importance of frequent and substantial risk reporting towards the executive and board level. The third research question deals with this matter. The same dimensions (content, frequency, timing and visual elements) that were discussed in the literature study are now investigated in practice.

#### 4.2.4. Determinants

**Research Question 4:** *Which organisational and/or contextual factors are influencing the risk oversight practices?*

The fourth research question deals with the factors that might influence the aforementioned risk oversight functions and systems. I expect risk oversight practices to vary from company to company. There is no one size fits all. One of the aims of this paper is to find organisational and/or contextual variables that help to explain the differences in risk practices. Possible determinants were mentioned in the previous paragraphs. The investigation might also reveal other influencing variables.

#### 4.2.5. Consequences of risk oversight

**Research Question 5:** *What is the impact of risk oversight on the company's results and level of risk taking?*

The last research question examines whether risk oversight practices actually have an impact on the organisation. This can be an influence on the financial results of the company or an influence on the corporate level of risk taking. Previous studies on the consequences of mature risk oversight practices were especially based on findings from financial organisations (Ellul&Yerramili, 2013). However, in this paper, research will be conducted in other industries.

### 4.3. Research methodology

#### 4.3.1. Research design

The empirical study is based on a qualitative approach. More specifically, I used a case study to generate findings on the risk oversight practices of Belgian companies. Case study research can be defined as: *“the in-depth study of instances of a phenomenon in its natural context and from the perspective of the participants involved in the phenomenon”* (Gall, Borg, & Gall 1996, p.545). I made use of a multiple case study design that consists of different individual cases. The evidence is more compelling compared to a single case study, which makes the overall study more robust (Yin, 2014).

I prefer a case study approach over a large sample quantitative study design for several reasons. First of all, case study research offers the benefit of having an in-depth understanding of a small number of cases in their real-world contexts which often results in new findings about a certain topic (Yin, 2014). Therefore, case study research provides me with comprehensive insights into the current state of risk oversight practices of a sample of Belgian corporations. Secondly, case study research is well suited for explanatory research (Yin, 2014). A study of multiple different cases will offer me insights into the determinants and consequences of risk oversight practices. Besides that, case study research is highly recommended when there is only limited knowledge available about a certain topic (Eisenhardt, 1989). Since little is known about the determinants and consequences of risk oversight in Belgian corporations, a case study is particularly suited for this topic. An inductive approach is used to develop a theory from the information gathered from the cases (Eisenhardt, 1989). Finally, this type of research offers the advantage of observing the variables in their natural setting and perceiving the general risk culture and mind-set of the organisations (Yin, 2009).

Case study research does not have a fixed format. However, one of its key principles is data triangulation or the use of multiple sources of evidence in order to increase the reliability of the results (Eisenhardt, 1989; Miles & Huberman, 1994; Yin, 2014). I chose to use two types of qualitative data. First of all, open-ended interviews are a commonly used source of evidence for case studies because of their high degree of flexibility (Yin, 2014). I therefore made use of semi-structured, in-depth interviews with Belgian companies to gather rich and extensive information on their risk management function. Secondly, I collected information from the corporate websites and organisational risk and/or corporate governance charters. Moreover, in 2004, there was the launch of the Belgian Code on Corporate Governance. This seriously increased the Belgian regulations on risk management for listed companies (Corporate Governance Committee, 2009). From that date onwards, organisations were obliged to publish information on their risk approach in their annual reports. Because of that, I could consult their annual reports to gather additional information.

#### **4.3.2. Target group**

Based on the findings of the literature study and the determinants mentioned in the theoretical framework, I put together a list of possible Belgian companies for my case study. Small and medium-sized enterprises mostly do not have formal risk oversight structures. I therefore decided to focus on publicly quoted and privately held Belgian companies of substantial size. I expect these companies to have a more advanced risk approach and more formal risk management systems. The study includes companies of a wide variety of industries in order to gain general insights in risk oversight. However, given the complexity of financial products, financial companies are subject to more stringent regulations. Given the lack of comparability, I decided to focus on non-financial companies.

In order to find potential listed companies for my case study, I made an overview of all the companies that are traded on the Belgian stock market. As a result, I obtained a list of 88 different companies. After excluding the financial companies, the list was reduced to 61 organisations active in a wide variety of industries. This list can be consulted in appendix 8. Concerning private companies, I searched for large organisations since I assumed that they are also consciously dealing with risk management.

#### **4.3.3. Sample selection**

The following step was to select a sample out of the extensive list of companies (Eisenhardt, 1989; Yin, 2009). I tried to contact as many of the companies on the list as possible by sending personal mails and short messages on LinkedIn. Every message consisted of a short explanation of the topic of my master dissertation and a short reasoning on why this specific company could be interesting for my case study. In order to contact the best person in every company, I made use of the information on corporate websites and LinkedIn. Moreover, I used the website of BELRIM to find possible interviewees within large Belgian corporations. BELRIM has over 200 members that are deliberately working on risk management. By attending the event of BELRIM in collaboration with the NBN (the Bureau for Standardisation) in February 2017 on risk management standards, I was able to gain some more insights into the current state of risk oversight in Belgian companies. Moreover, this event offered me the possibility to briefly introduce my research topic and establish the first contacts for the upcoming interviews. Since membership at BELRIM means that the organisation is deliberately working on risk management, these firms perfectly suited the profile as an interviewee for my case study. BELRIM also assisted me by sending an overview of my research project including the request for a short interview to a list of BELRIM members I selected in advance.

During the final selection of the cases, I also took into account the different determinants from my theoretical framework, to guarantee enough variety in the selected companies. Case study research does not prescribe an ideal number of cases, however 4 to 10 cases usually gather enough information to draw meaningful conclusions (Eisenhardt, 1989; Patton, 2002). Eventually, I conducted interviews with 8 Belgian companies. After the last interview, I reached theoretical saturation and possessed enough information to start my analysis (Eisenhardt, 1989). As I wanted to conduct interviews with the person who could provide me with comprehensive information on risk oversight, the function of the interviewee varied from company to company. Most of the interviews were conducted with the corporate risk manager, as these people are well-informed about the company's risk management. Despite the fact that they do not have a seat in the board, they could still provide me with comprehensive information on the risk role of the board. I made visits to the corporate offices to conduct the interviews. Table 1 includes a summary of the interrogated companies and the function of the corresponding interviewee. In order to respect their privacy, I do not mention the names of the interviewees. The last four organisations did not want to be mentioned by name. In order to distinguish the different organisations, I replaced their names by Company A, Company B, Company C and Company D. Appendix 11 also contains a summary of the interrogated companies and their key characteristics.

Company	Ownership	Industry	Interviewee
<b>Colruyt</b>	Publicly Listed	Retail & Wholesale	Corporate Risk Manager
<b>Proximus</b>	Publicly Listed	Telecommunications	Director of Audit, Risk and Compliance
<b>Raffinerie Tirlemontoise</b>	Private	Sugar Production	Director Legal Department
<b>Ardo</b>	Private	Frozen Food	Managing Director
<b>Company A *</b>	Publicly Listed	Digital Imaging	Corporate Risk Manager
<b>Company B *</b>	Publicly Listed	Information Technology	Internal Auditor
<b>Company C *</b>	Private	Aviation	Corporate Risk Manager
<b>Company D*</b>	Publicly Listed	Telecommunications	Corporate Risk Manager

*Table 1: List of Companies*

\* These companies want to remain anonymous.

#### **4.3.4. Interview approach**

The flexibility of an open-ended interview offers the advantage of revealing information that would have stayed unnoticed in an online questionnaire (Yin, 2014). In every interview, I made use of an interview guide in the form of a predetermined list of objective questions to exclude biases (Patton, 2002). After the first couple of interviews, small adjustments were made to the questionnaire to improve the quality of the gathered information. A Dutch and an English version of the final questionnaire can be found in appendices 9 and 10. It consists of well-defined questions in order to create a rich dialogue with the interviewees. The actual list of questions varied from company to company depending on the information that I gathered in advance from the firm's annual report and/or corporate website. Moreover, I allowed myself to deviate from the predetermined list and ask additional questions according to the interviewee's previous answers. The interviews were held in Dutch since it concerned Belgian companies.

In order to respect the busy schedules of the professionals, I limited the duration of each interview to approximately 45 minutes. I used a tape recorder in order to avoid interrupting the respondents during the conversation. It also provided me with a very accurate rendition of the interview (Yin, 2014).

## 5. Analysis

### 5.1. Methodology

In contrast to quantitative data analysis, qualitative data analysis has no fixed procedure to analyse the data (Yin, 2014). To draw meaningful information from the gathered data, I used a within case and cross case analysis (Yin, 2009; Miles&Huberman, 1994). First, I systematically organised the data in conceptually clustered matrices in accordance with the different research questions (see appendices 12 until 16) (Miles & Huberman, 1994). The companies are listed in the rows of the matrix, while the different topics associated with the research questions are listed in the columns. The boxes then contain findings and quotes from the interviews. The within case analysis focuses on the rows of the matrices, while the cross case analysis consults the information in the columns to answer each research question. I then considered every case as a separate study and afterwards I turned towards a comparative analysis of all the individual cases to find significant similarities and differences (Yin, 2014).

### 5.2. Within case analysis

The within case analysis contains an individual assessment of the companies. Every section starts with a brief description of the organisation. Additional key characteristics of each company can be found in the summary table in appendix 11. This matrix will be used in the cross case analysis when discussing the influence of the determinants. In the introduction of each case, I also mentioned the reason for selecting that certain company. Each analysis is then structured in accordance with the research questions, except for the question concerning the determinants of risk oversight, which will only be covered in the cross case analysis. In every case, the following six items are discussed: the company's attention to risk management, risk roles and responsibilities at executive level, risk roles and responsibilities at board level, SRM, internal risk reporting and finally the overall impact of risk management on the company.

### 5.2.1. Colruyt

#### *Company description*

Colruyt Group is a Belgian company active in the retail and wholesale industry. The company is listed on the Euronext Brussels Bel20 index. It is a family owned organisation, the Colruyt family and its relatives hold 51.88% of the shares. The group manages different sister companies such as Colruyt, DreamLand, Okay, etc. In 2016 the total revenue of the group amounted to €9.18 billion. The company was selected for this case study because of its large size and substantial amount of revenue. Moreover, the corporate governance charter clearly mentions that the group has set up RM and internal control systems based on the COSO framework. A large part of this charter is devoted to RM. Together with Colruyt's membership at BELRIM, this definitely indicates the high degree of interest in RM. Moreover, other companies referred to Colruyt's RM approach as one of the more mature of its kind. The interview was held with the corporate risk manager, accompanied by one of his associates in the risk office who is responsible for the group's RM programme.

#### *Attention to RM*

In 2005, a corporate risk manager was appointed for the Colruyt Group at the request of the chairman and in response to the increasing internal and external complexity. First of all, the chairman wanted to be more in touch with the business and its associated risks. Secondly, he asked for a higher risk awareness of all company members. Therefore, in 2009, he gave the order to the risk manager to develop an ERM programme for the group. Before 2009, risks were managed in a more emotional way, on gut instinct. The main goal of Coris, the Colruyt Group Risk Management programme, is to draw up an inventory of all the risks facing the company. It is based on the COSO framework (Colruyt Group, 2016). Under guidance of the RM team, every corporate domain has to identify and assess its own risks. Each domain has its own risk coordinator, who has to administer the risk register and make sure that there is enough attention to RM (Colruyt Group, 2016).

At this moment, Colruyt has a mature ERM system. Its key success factors are the high level of support from the top and the *"personal involvement on the field"* of the RM team. Employees receive guidance and training sessions to fully understand the risk approach. Colruyt has a risk-averse culture. The interviewee stated in this context: *"When it is your own money, and in a family business it is your own money, you will deal more carefully with risks"*.

#### *Risk roles and responsibilities at executive level*

Colruyt's RM team includes two people working on the Coris programme, 4 persons dealing with internal audit and one person responsible for compliance with the competition legislation. In 2010, this last person was added to the team in order to focus on the company's most important risk, namely the severe competition regulation. RM and internal audit have been combined in one department



since they both make use of the same skills and expertise. The corporate risk manager can be regarded as the firm's CRO. He is not a formal member of the ExCo, but he has direct reporting lines towards the CEO. As he also receives a high degree of support both from executive and board level, he stated that there is no need for a CRO position. *"As long as they (the ExCo and the board) don't need this function, neither do I"*. Because of the Coris programme, members of the ExCo now add RM to their periodic activity report. The CEO, who is also chairman of the board, gave the impetus for the risk programme.

#### *Risk roles and responsibilities at board level*

The demand for a more professional way of dealing with risks came from the chairman of the board. Moreover, he recruited a risk manager and asked for a corporate risk programme. This indicates that the board places great importance on RM. The chairman of the board is fully aware of the different risks facing his organisation. The entire risk approach is determined by an iterative process in close collaboration with the board. I quote the risk manager: *"One of the most important key success factors that determine whether your programme stands or falls, is the overall support, assistance, belief and mindset of the top. It is a sine qua non condition"*. Nevertheless, there is no separate risk committee at board level since this would overlap too much with the audit committee's responsibilities. The audit committee is mainly dealing with financial risks, while the entire board works on the strategic risks.

#### *SRM*

The business strategy is the foundation of the Coris programme. I quote the risk manager: *"When we carry out a risk identification session, we always start from the strategic objectives of the organisation"*. They try to identify issues which could prevent them from achieving the goals. One of the categories of the company's risk universe is 'strategic risks', such as market dynamics and regulations. The responsible for the ERM programme also mentioned that these risks easily emerge from the different domains.

#### *Risk reporting and provision of information*

The corporate governance charter refers to the company's *'extensive and advanced information and communication flows'* (Colruyt Group, 2016, p.149). Every business domain identifies its own risks. The RM team gathers all the information in the corporate risk register and then reports the results of the Coris programme and the key risks to the ExCo and the audit committee. The corporate risk manager has a direct reporting line towards the CEO, who is at the same time the chairman of the board, and towards the COO. He also has a link to the CFO, but this is rather for practical issues. Furthermore, he is accountable to the audit committee that in its turn reports to the board as a whole. However, since the risk manager firstly presents his findings to the board's chairman, the board is already informed before receiving the information from its audit committee. The reporting of the key risks to the top always happens on a quarterly basis. Concerning the operational units, the RM team expects an annual

review of the risk scores and at least a half-yearly follow-up. Risk matrices are used to determine the risk score based on its impact and likelihood. The company also has a risk universe which divides the risks into different categories such as financial, operational or legal risks. The risk manager stated: *“I can then push a button to see all the risks for a certain domain in a certain category”*. For every domain, the RM team reports on the risks, the different risk categories, the risk scores and their evolution.

#### *Impact of RM on the company*

Colruyt has a pragmatic approach, meaning that they implement systems based on their added value for the company and not because of compliance with regulations. RM is considered to be an important function because of its positive influence on Colruyt's operations. The actual impact of RM on the results is not measured, but they do examine the evolution of the risk scores. The risk manager stated: *“Our programme has sufficiently proven itself. Other companies are asking us how we handle that”*. The implementation of the Coris programme has also led to an increased internal awareness for RM. Employees receive a briefing in which the risk approach is described in an easy manner. In this way they are convinced of its positive results. The RM team is frequently contacted by other employees who want to appeal to their experience.

### 5.2.2. Proximus

#### *Company description*

Proximus is a Belgian company active in the telecommunications and ICT industry. It is the leading provider of telephony, internet, television and network-based ICT services to residential, enterprise and public customers in Belgium. In April 2015, the company's name changed from Belgacom to Proximus. The company is listed on the Euronext Brussels Bel20 index and is primarily state owned. The annual revenue of 2016 amounted to €5.87 billion (Proximus Group, 2016). Proximus definitely fits the profile as an interviewee because of its large size and its membership at BELRIM. Another reason for selecting this company is the substantial amount of RM information found in its annual report of 2016, which indicates the company's interest in RM. I conducted an interview with the Director of Audit, Risk and Compliance to gain more insights into Proximus' RM system.

#### *Attention to RM*

At Proximus, there has been interest in RM since the nineties. The company is truly convinced of the idea that taking risks is inherent to doing business. When risks are taken in a controlled manner, they might positively influence the company's return to its stakeholders (Proximus Group, 2016). According to the interviewee, the launch of the Belgian Code on Corporate Governance in 2004 and the general increase in attention to ERM has led to major changes in the firm's RM systems. It has also led to a growing awareness for RM over the years. In 2006, RM merged with the internal audit function into one department to create more synergies. Nowadays, the company constantly tries to improve its RM by comparing to best practices of other Belgian and European organisations. The interviewee stated: *"We recently came together with Colruyt, UCB, Engie and Solvay to see where we are in terms of maturity and to verify whether our ERM model, which dates back from 2007, is still working well"*.

Proximus' ERM programme is based on the COSO framework. The annual report contains a description of each of the 5 areas of the COSO methodology. At this moment, Proximus' RM focuses on three key areas: business continuity, performance and data security & privacy. This last topic is becoming increasingly important because of the forthcoming introduction of the European General Data Protection Regulation (GDPR).

#### *Risk roles and responsibilities at executive level*

Proximus has no formal CRO position at executive level. However, the Director of Audit, Risk and Compliance (ARC), who is just below the executive level, is often seen as the CRO of the company. The support from the top is guaranteed by a direct reporting line towards the Chief Corporate Affairs Officer (CCAO). Together with other members of the ExCo, he takes the decisions concerning the company's risk appetite.

Proximus has appointed a RM and Compliance Committee (RMC) at executive level that consists of the CCAO, the CFO and the Chief Strategic Officer. The main objective of this committee is to oversee the key risks and how they are being managed. The committee holds quarterly meetings to discuss the company's risk philosophy in relation to the strategy and make decisions on critical risks by finding the balance between risk taking and the associated costs. The group has four general strategies at its disposal to decide on risks: avoid, transfer, reduce or accept the risk (Proximus Group, 2016).

#### *Risk roles and responsibilities at board level*

The interviewee stated: *"RM is very important for the board because in the end, the ultimate responsibility for the company rests with the board members. Therefore they have to be fully aware of the risks facing the firm"*. The Director of ARC provides the board with information on ERM and he mentioned that the board is involved in RM. It is their task to assess the effectiveness of the internal control and RM systems (Proximus Group, 2016).

Proximus has no separate board level risk committee since its benefits would not outweigh the additional costs. In accordance with the corporate governance laws, the company has a board level Audit & Compliance Committee (A&CC). This committee has to advise and assist the board on its tasks relating to RM and compliance. The A&CC holds at least quarterly meetings (Proximus Group, 2016). According to the interviewee: *"The company's internal audit is risk-based, meaning that RM has a large influence on the audit plan and objectives"*.

#### *SRM*

Proximus has a structured and consistent ERM framework in place to assess and respond to risks that could have an impact on the achievement of its strategic objectives. The interviewee stated: *"ERM gives a clear overview on all organisational risks, both operational and strategic uncertainties and opportunities"*. According to the annual report: *"The Group's ERM seeks to maximise value for shareholders by aligning RM with the corporate strategy"* (Proximus Group, 2016, p. 34) and *"Risk assessment and evaluation takes place as an integral part of Proximus' annual strategic planning cycle"* (Proximus Group, 2016, p. 34). The company develops a three year strategic plan and subsequently identifies the risks, uncertainties and opportunities associated with this plan. I quote the interviewee: *"SRM is the number one priority of this organisation"*.

In order to identify the strategic risks (competition, regulation, ...), Proximus carries out an annual survey. In the first part, interviews are conducted with approximately 70 directors, high potentials and the strategic department in order to rank the risks based on their priority. The second part of the survey is held at the level of the BUs, departments and affiliates to discover their critical risks and uncertainties. The findings of both parts of the survey are then used as an input for a workshop at BU

level. This workshop should help to discover the most important disruptive events in order to determine the necessary mitigating actions. According to the interviewee, *“Everything is strongly linked with the business strategy”*. Recently, the template of the survey has been renewed to improve the quality and reliability of the findings.

#### *Risk reporting and provision of information*

*“Proximus has a tradition of a strict adherence to a timely and qualitative reporting”* (Proximus Group, 2016, p.43). Both the Director of ARC and the RM and Compliance Committee (RMC) report directly to the CCAO at ExCo level and the A&CC in the board. *“The resulting report on major risks and uncertainties is then reviewed by the Executive Committee, the CEO and the Audit and Compliance Committee. The main findings are communicated to the Board of Directors”* (Proximus Group, 2016, p.34). There is a high degree of internal communication with weekly meetings and a lot of face-to-face contacts between the Director of ARC and the ExCo level. The director also attends the quarterly meetings of the audit committee to provide the members of an elaborated risk opinion.

Proximus uses risk scorecards to provide information on each risk. These scorecards indicate the probability and impact of a risk, the velocity, the involved BU level, mitigating actions, KRIs, early warning systems and the risk owner. In the future, the company would like to increase the use of these comprehensive scorecards to present risk information in a more coherent and transparent way.

#### *Impact of RM on the company*

The combination of RM with the internal audit function creates a lot of synergies for this company. In case of a serious risk, an internal audit can be implemented. In the past, the organisation was especially focused on risk insurance and prevention. Since 2006, a lot of progress has been made by linking the RM function with the business strategy and increasing the attention to ERM. According to the interviewee: *“Solely focusing on operational risks does not suffice”*.

### 5.2.3. Raffinerie Tirlemontoise

#### *Company Description*

Raffinerie Tirlemontoise is a private Belgian company that produces a broad range of sugar products. In 2015, the company had a turnover of approximately €530 million. In 1987 the company decided to register 25% of its shares on the Brussels Stock Exchange. The other 75% of the shares were bought by the German group Südzucker. In 1989, Südzucker obtained the remaining 25% that was traded on the stock market by a public offer. The group thereby obtained the full ownership of the company (Raffinerie Tirlemontoise SA, 2015). This company has been selected because of its substantial size and its membership at BELRIM. The interview was conducted with the director of the legal department.

#### *Attention to RM*

In 1982, Raffinerie Tirlemontoise was hit by a massive explosion in one of its sugar factories. This disaster killed three employees and many others got injured. At that moment, the company appointed a safety manager who carried out an internal risk assessment. Based on his findings the company then installed a programme to increase its safety level. Whereas the company used to solely focus on operational RM in the past, they are now paying increased attention to strategic risks.

#### *Risk roles and responsibilities at executive level*

The RM responsibility is spread across the organisation. Every plant has its own prevention consultant who determines and manages his own risks. The legal director is the final responsible for the company's RM and has to manage the company's risk portfolio. He is a member of the executive board. Before 2005, when the company was still allowed to determine its own risk strategy, he even had the title of corporate risk manager. However, as from 2005, RM became a group function led by the executive board of Südzucker. By integrating the RM departments of its subsidiaries, the group wanted to create more synergies. The interviewee stated: *"The strategy, guidelines and procedures for RM are now completely determined by our parent company"*. He also mentioned that Südzucker attaches considerable importance to effective RM. This is also confirmed by the fact that approximately 15 pages of Südzucker's annual report are devoted to RM (Südzucker, 2016). There is no CRO appointed in the company because RM is already controlled by the parent company.

#### *Risk roles and responsibilities at board level*

The board of Raffinerie Tirlemontoise is entirely composed of German delegates of Südzucker. Board members receive risk information from their CEO, as well as from the RM department of Südzucker. Since the risk strategy is already being determined by the parent company, the RM role of the board of Raffinerie Tirlemontoise is rather limited. Hence, there is also no separate risk or audit committee. By contrast, Südzucker's board has appointed a separate risk committee to give proper consideration to the group's RM. An overview of Südzucker's RM system can be found in appendix 15.

### *SRM*

The interviewee stated: *“RM has evolved from pure operational, ..., to the assessment of risks of investments, new products, etc.”*. This illustrates the company’s increasing attention to strategic risks. When in 2005 the operational RM was taken over by the parent company, Raffinerie Tirlemontoise started to focus more on SRM, an upcoming trend at that time. I quote the interviewee: *“In my view ERM is a hot topic”*. Südzucker’s RM department identifies the strategic risks facing the group and describes them in its annual report (Südzucker, 2016). Moreover, every director of the Raffinerie Tirlemontoise has to map the strategic risks in his own area. The executive board then quarterly comes together to discuss new projects and acquisitions. They examine their feasibility and expected return by taking into account the associated risks. Nevertheless, the company does not list the different risks in a register and at this moment, it has no formal ERM programme in place. According to the interviewee, formal systems will only be developed in response to a request from Südzucker.

### *Risk reporting and provision of information*

Operational RM is carried out in close collaboration with the different plant managers. They report their risks to the company’s safety and environmental coordinator, who in his turn informs the director of the legal department. The legal director then has to combine and analyse the received information. Afterwards, during executive board meetings, these topics are discussed and the legal director then informs the CEO on the current state of RM. Reporting towards the CEO happens approximately two or three times a month, mainly through personal communication. Moreover, the legal director reports indirectly towards his German colleague of Südzucker. The board of Raffinerie Tirlemontoise receives its information from the CEO and the RM department of Südzucker. The legal director also attends the quarterly board meetings, since he is at the same time the board secretary. He is often asked to provide additional information on certain topics. Finally, the company is aware of the existence of visual tools to support the reporting process but does not use them at this moment.

### *Impact of RM on the company*

The interviewee stated that they have no clear view on the added value of RM. The company does not measure the costs and benefits of risk mitigating actions. Nevertheless, they assume RM has a positive influence on their operations since there were less accidents. Furthermore, they continuously run a campaign to raise employees’ awareness for RM. This programme definitely pays off as they see a significant impact on the internal risk culture. It was also confirmed that the company is becoming more risk averse. Whenever possible, they try to avoid or reduce risks.

#### 5.2.4. Ardo

##### *Company description*

Ardo is a family owned business that is the European leader in the frozen food industry. Its customer database consists of retail, foodservice and industrial clients. The company has production and distribution facilities in 9 European countries and sells its products in 58 different countries worldwide. In 2016 Ardo had an annual revenue of €868 million. The main reason to include Ardo in this case study is to discover whether there is a significant difference between listed and private companies in terms of RM. The second reason for selecting Ardo is its large amount of revenue. Given its' substantial size, I assumed that Ardo would also have formal RM systems in place. Ardo is not publicly listed and thus not obliged to publish a comprehensive annual report. I could therefore only rely on the data from the interview to analyse this case. The interview was conducted with the managing director.

##### *Attention to RM*

As from the establishment of the company in 1977, Ardo has taken into account the risks related to its business operations. The managing director referred to his company as *"very risk averse"* and he mentioned that every decision in RM has to be preceded by a careful consideration of the associated costs. Nevertheless, the interviewee also stated that sometimes certain well-considered risks should be taken because they might offer benefits for the company. Ardo's RM function is not based on a theoretical framework or specific system. The interviewee stated: *"That would be too formal for our company"*. Instead, the company has some internal rules and procedures to guide the decision-makers in RM. These documents are a product of years of experience with reoccurring risks. The most important risks facing the firm are the varying prices of raw materials, currency risks, the fluctuation in energy prices, etc. Ardo tries to come to agreements with its suppliers to set fixed prices for a certain period of time. Overall, Ardo mainly uses long-term contracts and a geographical distribution of activities to reduce the level of risk.

##### *Risk roles and responsibilities at executive level*

In contrast with the previously discussed cases, Ardo has no formal roles or specific structures devoted to RM. Instead, every department has to assess and manage its own risks. For instance, risks related to the purchase of food and risks related to the purchase of non-food materials are being managed in different departments. According to the interviewee: *"Every risk is different, so every division has its own approach"*. The divisions report their key risks to the ExCo to guarantee that the executive level is at any time aware of the major risks. The ExCo is composed of Ardo's CEO, the managing director and the COO. They are held responsible for the corporate strategy, investment decisions, budgets and the supervision of all operational activities (Ardo, 2014). Moreover, based on the risk information they receive, the ExCo has to take decisions on contracts and mitigating actions. The interviewee stated:



*“Especially for the most important risks, such as financial risks and risks related to raw materials, all decision-making is centralised”*. There is no executive level risk committee or CRO in Ardo. It is the ExCo as a whole that has to oversee the company’s risks. Up until now, Ardo’s audits were performed by an external auditor. Recently, the company has started an internal audit function. This department is still in its early phase and is not involved in RM. However, this might change in the future.

#### *Risk roles and responsibilities at board level*

Ardo is a family owned company and its board is almost completely composed of family members. Because of the fact that the board and the ExCo are composed of members of the same family, there is a very high degree of informal information exchange and transparency. Moreover, the tasks and responsibilities of these two levels might sometimes overlap. The ExCo always has to disclose the key risks, such as financing risks and currency risks, to the board. Together, both levels have to come to agreements on different strategies to manage the key risks.

#### *SRM*

When asking whether risks are being identified in close connection with the corporate strategy, the managing director stated: *“No, every department has to determine its own risks. This is not directly established based on the strategy of the firm”*. This shows that the company currently does not operate according to the principles of SRM. Of course, key risks are implicitly related to the business strategy.

#### *Risk reporting and provision of information*

Every division discloses its risks to the ExCo which in its turn presents the key risks to the board of directors. A major part of the information provision happens in an informal way because of the close family ties between the executive and board level. The managing director stated: *“All shareholders know the company and everything is being discussed in an informal way. We do not really make use of formal reporting systems”*.

#### *Impact of RM on the company*

According to the interviewee, Ardo is active in a quite stable industry, *“The food sector is quite stable since people no matter what continue consuming”*. Furthermore, Ardo mainly makes use of a natural way to cover its risks. For instance, by spreading its activities across different countries, the company is less dependent on the circumstances in one specific country. Other arrangements include the spreading across different types of vegetables and fruit and the company’s highly diversified customer base. Other risks are being reduced by negotiating fixed prices with suppliers or customers. The result of all this is that Ardo’s results are relatively stable.

### 5.2.5. Company A

#### *Company description*

The name of company A will not be disclosed in order to respect the confidentiality agreement. The company is active in the IT and digital imaging industry and is listed on the Euronext Brussels BEL20. In terms of size, this company fitted the profile as an interviewee since it had an annual revenue in 2016 of more than €2.5 billion. Moreover, the interviewed risk manager is member of BELRIM and FERMA. When looking into the annual report of 2016, it immediately becomes clear that the company attaches major importance to RM. The corporate governance statement describes how RM is being implemented in the organisation and gives an indication of the key risks.

#### *Attention to RM*

Shortly after going public on the Euronext Brussels in 1999, one of the board members, the former rector of the KU Leuven, introduced RM in the organisation. According to the corporate risk manager *“The company was one of the first Belgian organisations that was consciously dealing with RM”*. In contrast with other organisations, there was no need to convince the board or ExCo of its importance since RM was imposed from the top. In the beginning, everything had to go exactly as how it was prescribed by the theoretical guidelines because of the academic influence of the KUL. According to the interviewee, this was too ambitious and they therefore decided to solely focus on those risks that might have a substantial impact on the results. This new approach, together with the conversion of the company to other activities, strongly reduced the initial resistance from other functional departments. I quote, *“At that time, I quickly gained support from people on the field”*. The company's RM was and still is based on ERM with a formal system based on the Australian Standards. They try to apply standard methodologies and procedures throughout the entire organisation. However, this is sometimes difficult given the different countries and cultures in which the firm is operating.

#### *Risk roles and responsibilities at executive level*

The organisation is highly vertically controlled with all operations reporting to and being assessed by a small corporate management team. Members of this team get a lot of support from the board and the ExCo. The corporate risk manager is part of this team and is responsible for RM and insurances. He stated: *“Insurance management is a tool to manage risks but it is not an end in itself”*. The sector in which the company is active is subjected to strict regulations. Therefore multiple executive committees have been installed that are responsible for business continuity, security, quality etc. These committees are all dealing with risks and uncertainties in their own area. However, they are not referred to as official ‘risk committees’.

The corporate risk manager repeatedly mentioned the high degree of transparency between board and executive level and the board's strong support for RM. But in the end, it is the ExCo who has the

most active role in the RM of the firm. The annual report mentions that the ExCo frequently identifies and assesses risks and has to inform the audit committee on the key risks. The CFO is ultimately responsible for RM at the executive level. Up until now there has been no need to appoint a CRO, since the risk manager is *“only a telephone call away”* from the board and the ExCo. A CRO is often nominated in organisations to increase the support of RM from above. However, in this case, RM is already highly supported from the top. The interviewee mentioned that this was possibly going to change within a few years from now when he would leave the company.

#### *Risk roles and responsibilities at board level*

For this company, the board is more than an advising body, it has a very active role. The interviewee referred to the board as a *“coach”* or *“partner”* for the organisation. The board also has a very active role in RM, which is not surprising knowing that the initial demand for RM came from the board. The annual report of 2016 mentions that the board develops the business strategy in close collaboration with the RM function and it also decides on the company’s risk appetite. Moreover, the board is held responsible for evaluating the RM function.

In 2003 the company appointed a risk committee at board level. To guarantee the segregation of duties, this committee was chaired by the CFO, while the audit committee was chaired by the CEO. The risk committee could be situated just below the board level. A decade ago, concerns were raised about the duplication of responsibilities and reporting lines between the audit and risk committee. At that moment, they decided to merge these two committees into one committee, the audit committee. According to the latest annual report, it now consists of three non-executive members. The committee holds at least four meetings a year to discuss audit and RM matters. I quote the corporate risk manager: *“The internal auditor and I are on the same hierarchical level in the firm. In many companies, the internal auditor is the risk manager’s boss. However, in this company, we work together”*. The risk manager and internal auditor are referred to as *“the good and the bad”*. I quote the interviewee: *“Internal audit and RM cannot be separated from each other”*.

#### *SRM*

The board considers RM as a support function to put the strategy into effect. I quote, *“A risk manager has to support the global strategy of the company”*. In this company, the development of the strategy happens in collaboration with RM to discover the risks and uncertainties associated with the business plan. Nevertheless, this process is not always carried out as it should be so there is still room for improvement in the area of SRM at Company A.

#### *Risk reporting and provision of information*

The interviewee stated: *“The corporate risk manager is an independent function with easy access to the top”*. He reports directly to the CFO. Because of the very open and accessible company culture, a

lot of risk reporting happens in an informal way. The risk manager stated: *“In case of a board meeting, we always have to be stand-by”*. He thereby means that he is often called to provide board members of additional risk information during a meeting. This again happens in an informal way.

The company also has some formal reporting practices. The audit committee reports on a quarterly basis to the board on internal audit and RM. In the past there were separate reporting lines for internal audit and RM. However, since the combination of these two committees into one, risk information is a systematic part of the audit report to the board. The use of visual tools in formal risk reporting is limited to the discussions in the different executive committees. At this moment, reporting towards the ExCo and the board does not include such tools. The company would like to improve this in the future to make the reporting practices more professional.

#### *Impact of RM on the company*

The company has a very mature RM function, mainly because of the fact that they already built up a lot of experience over the years. Therefore, they are often a step ahead of new regulations which saves them investment costs. Throughout the entire organisation, everyone is aware of the importance of RM. This is visible in the way people are paying attention to risks and prevention. Nevertheless, the company's head start also has the disadvantage of having very traditional and sometimes outdated methods. According to the interviewee, *“The administrative approach could be improved”*. In the future, he would like to work with an online system that is automatically updated when a risk status changes.

### 5.2.6. Company B

#### *Company description*

The name of company B will not be disclosed in order to respect the confidentiality agreement. Company B is a Belgian company that provides ICT services to corporate customers in Belgium and beyond. The firm is noted on the Euronext Brussels BEL20 stock index. The annual report of 2015-2016 disclosed an annual revenue of more than €230 million. First of all, this company fitted the profile as an interviewee because of its stock exchange listing and its annual report mentioning the importance of RM. Secondly, it is a very interesting case because of the smaller firm size compared to other listed companies in this study. The interview was conducted with the internal auditor since there are no risk managers appointed. Moreover, this person is most familiar with the company's RM function.

#### *Attention to RM*

Since its merger in 2005, RM is described in the company's corporate governance charter. However, in practice, RM was and still is rather implicitly present in the company. Some loss-making projects in the past have increased the firm's awareness for RM, mainly in the area of project management and tenders. Recently, a risk management policy for project-related risks has been developed. This policy includes a definition of the risk roles and responsibilities, the categorization of risks, actions, structures and reporting practices. The interviewee stated: *"In fact it is our intention to extend this policy to other areas, but this step has not yet been taken"*.

Another important determinant for the recent increase in significance of RM is the importance of data management in the sector. The company is subject to very strict European regulations on data privacy and security. Especially the forthcoming GDPR will have a strong impact on the company's operations and RM function. New procedures and systems will have to be implemented in the company in order to comply with the new European regulation.

#### *Risk roles and responsibilities at executive level*

The final responsibility for RM rests with the ExCo and the board. Nevertheless, there are no formal roles appointed neither on executive level nor on board level. RM is a responsibility of the internal auditor and the company's operational management since there is no independent RM department. According to the interviewee, the secretary general can be seen as *"the point of contact for RM"*. He is part of the management committee and is the secretary of the board and the audit committee. He assists the executive management with the internal organisation of RM and contacts with the board. The secretary general is held responsible for the compliance with corporate governance principles and for the effective functioning of the board and its committees. Furthermore, the CFO is also indirectly involved in the RM process as he has to guarantee a proper budgetisation for the company.

### *Risk roles and responsibilities at board level*

According to the annual report of 2015-2016, the board supervises the implementation of the internal control and risk framework that has been developed by the executive management. The corporate governance charter in its turn indicates that the board has to decide on the risk appetite. However, according to the interviewee, the board's role in terms of RM is rather *"supervisory, controlling"*. While the board as a whole has the final responsibility for RM, part of it is delegated to the audit committee. This committee is composed of 4 independent and non-executive members that meet at least quarterly. Their main task relating to RM is to oversee the process and advise the board.

Normally, the board and the ExCo should carry out the risk assessment allowing the audit committee to rely on this information for its activities. However, the interviewee stated that this only happens at a very irregular basis. *"Therefore, the audit committee itself took the initiative to carry out a risk assessment"*. At this moment, the internal auditor is conducting approximately 20 interviews at managerial level to evaluate the organisational processes on their maturity. During this process he captures the most important risks by combining different insights. His findings are reported to the ExCo and the audit committee. I can conclude that the risk role of the board in this company is rather limited as they are not systematically identifying the risks facing the company.

### *SRM*

Despite the importance of strategic risks in the industry, the same concern applies to the area of SRM. The company has an advanced strategy process at its disposal, but this is not always systematically followed. Rather than deciding on the strategy apart from the financial decisions, the strategy and budgetisation process are often overlapping. At board level, the attention to risks and uncertainties during the strategy process is rather limited. According to the interviewee, there is still a lot of room for improvement relating to SRM.

### *Risk reporting and provision of information*

The internal auditor identifies risks in order to develop a risk-based audit plan. To present a clear overview, he draws up a list of all organisational processes and their current risk profiles, impact, probability, risk owner, etc. He thereby makes use of different visual tools such as colours to indicate maturity levels and risk profiles. I quote the internal auditor: *"If I would present too much information, a big part of it would go to waste"*. Therefore, he has to select the key risks to be reported to the higher organisational levels. He also stated: *"In the hierarchical structure of the company, I report my findings to the general manager. However, functionally, I report towards the audit committee in order to guarantee the independence of our function"*. He reports on a quarterly basis to the audit committee, which in its turn reports the key points to the board.

The secretary general is not included in the reporting line. Nevertheless, as secretary of the board and audit meetings, he is always informed of the latest findings of the internal auditor. During board meetings, RM is implicitly being discussed at the development of the strategy and budget management. There is no special time reserved to discuss the key risks and their impact on the operations. This again indicates the lack of formal attention of the board for RM.

#### *Impact of RM on the company*

The interviewee mentioned that it is difficult to measure the impact of RM on the organisation. According to the CEO, RM sometimes has the opposite effect of a substantial increase in risk aversion. Especially when the focus is on loss-making projects, the internal willingness to take risks seriously decreases. However, taking positive, calculated risks can also come with great rewards. The interviewee mentioned that the use of a risk portfolio would help the company to ensure a proper balance as it would give an indication of the current risk profile and risk appetite.

Overall, the interviewee believes that the company's RM might benefit from a more formal approach. *"At this moment, the company lacks systematic and regular practices in RM"*. More support from executive and board level could also assist in increasing the importance of the RM function.

### 5.2.7. Company C

#### *Company description*

Company C is active in the aviation industry and is privately held by the Belgian State (25%) and other private investors (75%). It has an annual revenue of €497 million. The company perfectly fitted the profile as an interviewee because of its substantial size and its large amount of added value for the Belgian economy. It is the second most important economic growth pole in Belgium. Moreover, the company's membership at BELRIM and FERMA (Federation of European Risk Management Associations), definitely shows that it is highly committed to RM. The interview was conducted with the corporate risk manager. He was honoured in the first 'Excellence in RM Awards' organised by FERMA for the company's Innovative Insurance Programme (FERMA, 2016).

#### *Attention to RM*

When the former CFO became CEO in 2010, he created the RM department. Both the internal audit and the newly appointed CEO wanted to pay more attention to RM. The RM department solely consists of the corporate risk manager: *"I monitor all the corporate risks, those risks that transcend the departments"*. His main task is to consolidate the risks and examine their interrelationships. In 2013 the RM function has been combined with insurance management. In 2017 an additional department for compliance and business continuity was created to guarantee the company's continuity. This compliance function especially deals with the institutionalised risks by way of operational inspections or *"ticking the box checks"*. Everything has to be compliant with the Belgian and European legislations.

#### *Risk roles and responsibilities at executive level*

The company has no risk committee or CRO at managerial level. However, I quote the interviewee: *"You could say that our CEO is the CRO"*. The CEO is the final responsible for the RM function and has delegated this function to the CFO, who in its turn delegated it to the risk manager. When having a look at the corporate organigram (see Appendix 17), RM is situated under the finance division. The risk manager stated that at this moment, the company does not really need a CRO since he would only manage the risks of other people, without having his own tasks. The interviewee repeatedly pointed at the important role of the ExCo. *"Everything stands or falls with the directorate"*. He mentioned that the CEO drafts the proposals on the risk appetite and risk approach.

#### *Risk roles and responsibilities at board level*

The interviewee was very clear on the board's role in RM: *"The impact of the board on RM is extremely limited"* and *"The centre of gravity of RM definitely does not lie with the board"*. Everything is presented to the board members and all they have to do is give their approval. As the firm has no separate risk committee at board level, it is the audit committee who deals with RM. Nevertheless, in the same way as for the board as a whole, the committee's only task is to receive reporting.



### SRM

The corporate risk manager mentioned that he particularly focuses on strategic risks. He believes that the company already has a strong position in this field. Recently, the company introduced its strategic plan. The risks associated with this strategic plan have immediately been incorporated in the internal risk register. The new ISO standards also ask the company to identify risks based on the business strategy.

### *Risk reporting and provision of information*

The risk manager identifies the risks facing the company by interrogating company members. The detected risks are then incorporated in the risk register on the internal network. Afterwards, the risk manager quarterly presents the top 10 or 20 towards the CFO and CEO. He thereby makes use of clear colour codes and risk scorecards. Every risk is depicted on two axes measuring the impact and the likelihood on a scale of one to five. This happens for both the inherent and the managed risk in order to clearly monitor the evolution. The CFO and CEO quarterly report the risk information to the audit committee which in its turn presents the risks to the entire board. The risk manager also attends the audit committee. Nevertheless, he is only allowed to stay for the risk presentation itself. In his opinion, presence during the entire committee would increase the amount of information he receives. Another weakness in the reporting system is the company's pursuit of overall consensus. Risks are often removed from the list due to only a few people who disagree. At this moment, the company is working on an improved information flow by adding more structure to the reporting systems.

### *Impact of RM on the company*

RM is really important for the credit rating of the company because the company issues bonds. A substantial part of the offering circular deals with the company's risk approach. I quote the interviewee: *"A strong RM function is increasingly recognised"*. The credit rating agency's report also mentioned the company's resilience or high capacity to overcome challenges. According to the interviewee, there was also a substantial increase in the internal awareness for RM. *"Colleagues are more likely to come to me and they appreciate my contribution"*.

### 5.2.8. Company D

#### *Company description*

Company D is a Belgian company active in the telecommunications industry. Since 2005, the firm is listed on the Euronext Brussels Bel20 Index. An American telecommunications concern, holds more than half of the shares. In 2016 a revenue of more than €2 billion was generated. Company D was selected for this case study because of its large firm size and its attention for RM. The annual report of 2016 clearly mentions that it has implemented RM and internal control systems in order to meet its RM objectives. The interview was conducted with the corporate risk manager.

#### *Attention to RM*

Ever since its foundation in 1996, Company D has paid attention to RM. In 2005 there was a serious increase in awareness for RM because of the firm's entry on the stock market. Since then, Company D is fully compliant with the provisions of the Belgian Code on Corporate Governance. There was, for instance, the creation of a board level audit committee. Another important event occurred in 2007, when a large U.S. company became the majority shareholder of Company D. Since the U.S. company has to be compliant with the U.S. SOX regulation, they forced Company D to develop a risk control framework. This ERM system is based on the COSO framework and led to the foundation of an executive level RM department. The interviewee stated: *"It stressed the importance of internal control and indicated that it should take place in a more formal way"*. At this point, Company D is continuously trying to improve its RM.

#### *Risk roles and responsibilities at executive level*

Overall, the structure of Company D's RM is based on the Three Lines of Defense Model. The first line includes the functions that manage and own risks in the company's daily operations, called *"the business"*. The second line includes the functions that are specialised in RM and oversee the risk practices, being the executive level RM department. Finally, the third line comprises the internal audit function, which has an independent monitoring role. This function is performed by the internal audit department of the U.S. company. Based on the feedback from the first two lines, the audit function implements internal controls and develops the audit plan.

Company D's RM structure is highly decentralised. The ownership for the different risk areas is spread across the functional departments. The executive level RM department was created as a central oversight function. I quote the interviewee: *"To make sure that the different risk areas speak the same language"*. The RM department is held responsible for monitoring the risks and for implementing controls to make sure that all risks are covered. It clearly appoints the risk owners and makes recommendations for mitigating actions. Furthermore, the interviewee mentioned that Company D's RM and compliance department often overlap. This is also mentioned in the annual report: *"The RM*

*department and the compliance function work closely together...*". Therefore, the interviewee believes that combining the capabilities of these two functions into one new department could create synergies.

The final responsibility for RM in the ExCo belongs to the CFO as there is no separate CRO position. The interviewee mentioned that he would like to have more support from the top. According to him, the appointment of a CRO would help to achieve this goal since *"as member of the ExCo, he would have a greater participation and draw more attention to RM"*. This would increase the amount of resources allocated to RM, particularly important in the context of the forthcoming European privacy regulations.

#### *Risk roles and responsibilities at board level*

The key role of the board in RM is to verify management's actions. Furthermore, board members decide on the company's general risk profile and risk appetite. Company D has no formal risk committee at board level. According to the interviewee, this is *"over-ambitious for the company"* and *"there is insufficient support"*. Instead, its audit committee has to assist and advise the board on RM and internal control. The committee annually reviews the company's RM systems and control procedures. Their role is particularly an advising one, with the final responsibility for RM remaining with the board as a whole.

#### *SRM*

At Company D, it is the ExCo who sets out the strategy. The board has a more controlling function, meaning that it has to verify whether the strategy is in line with the shareholder's expectations. At this moment, the company is carrying out an ERM exercise driven by the external demand for more attention to strategic risks. The interviewee stated: *"Such matters rise and fall depending on the support you get from the ExCo"*. Company D's board and ExCo rather prefer *"a light approach"*, meaning that they want to devote time to ERM, but they do not call for a comprehensive and formal system. I can conclude that the company is definitely aware of SRM, but more support from the top is needed to secure better implementation.

#### *Risk reporting and provision of information*

Company D has a centrally managed data warehouse and repository with information on internal controls and associated actions to provide the leadership team with relevant risk information. Important issues are saved in this repository and are subject to a monthly follow-up. The risk department at executive level reports towards the CFO and the board level audit committee. Reporting towards the CFO does not happen very frequently. According to the interviewee, *"The CFO is just part of the standard reporting lines"*. The audit committee receives a quarterly risk report, which includes presentations, written information and financial reports.

Company D has a risk and control matrix for every important key risk area to have a clear overview on its evolution. These matrices are far too detailed to present to the audit committee. During the audit meeting, risk managers prefer to use other visual tools such as risk or assurance maps and comprehensive risk scorecards. An assurance map visualises the different risks of each area with their associated maturity level, as well as an evolution of the risk score over time and the date of the last audit on this area. For every individual risk, the company maintains a risk scorecard. This card mentions the risk owner, the initial amount of issues, the evolution of the risk score, etc.

#### *Impact of RM on the company*

The major impact of the recent changes in RM is situated in the minds of the people at the organisation. There is an increasing awareness for RM and people start to realise that more formal roles and systems are needed for effective results. Furthermore, new systems and practices have an influence on the operational results of the company. For example, the structured RM approach in the area of revenue and fraud discovered a lot of revenue leakage. The same approach is now being implemented in other areas of the company. Benefits of new systems mainly occur during the first years of implementation as the marginal advantages decrease over time. Nevertheless, since a lot of RM activities are rather preventive, their results are not always visible.

### 5.3. Cross case analysis

The cross case analysis combines the findings of the individual cases to draw overall conclusions about the current state of risk oversight in Belgian companies (Yin, 2014). Besides looking for similarities, I also focused on remarkable differences between the cases to either confirm or disconfirm the predetermined assumptions. The analysis is structured in accordance with the different research questions.

#### 5.3.1. Risk oversight structure and responsibilities

The first research question concerns the allocation of risk management roles and responsibilities at executive and board level in Belgian corporations. As assumed in advance, no two companies have the exact same risk oversight structure. Nevertheless, I noticed a lot of similarities when structuring the data in a matrix (see Appendix 12).

Four of the eight interviewed companies have a separate RM department or team that oversees the company's risks. The corporate risk manager almost always presides over this team. It mainly concerns organisations with more mature RM systems. Their risk ownership is spread across the entire company, meaning that every department has to identify and assess its own risks. The RM department then operates as a central oversight function and monitors all the risks and their interdependencies. It is often combined with other corporate functions such as internal audit, compliance management or insurance management, or the company considers a future merger with another department to create synergies. At Company C, the RM department is composed solely of the risk manager. Companies that do not have a separate RM department, by contrast, have a single individual responsible for RM.

The main responsibility for RM rests in most organisations with the executive committee which is in its turn controlled by the board. The risk responsibilities of the executive level usually include the determination of the overall risk approach, the development of RM systems and the decision on the risk appetite in accordance with the business strategy. At Colruyt, Company A and Company C, the incentive for RM even came from the ExCo and the board. Despite the high interest in RM, none of the interrogated companies have formally appointed a CRO in the ExCo. Moreover, Proximus is the only company that has installed a RM committee at executive level. Company A has different executive committees who all deal with their own specific risks. Leadership in RM is almost always assigned to an existing corporate position. Two companies stated that their CFO can be regarded as their CRO, while others referred to their CEO, corporate risk manager, legal director or secretary general to fulfil this role. Despite the variation in the designated functions, five companies provided a similar explanation. They stated that they do not need a CRO because of the already high level of support

from the top and/or the direct reporting lines towards top management. The RM of Raffinerie Tirlemontoise, for example, is completely controlled by its parent company Südzucker. Therefore, they do not need an internal CRO. Company D, by contrast, stated that appointing a CRO could be helpful to strengthen the support from the top.

The risk role of the board of directors is mostly based on a close collaboration with the executive management. While the ExCo usually submits proposals on the risk strategy and appetite, the board has to approve them and take the final decisions. In addition, they supervise management's actions and assess the effectiveness of the company's RM. Four out of the eight companies explicitly mentioned that their board attaches considerable importance to a professional risk approach. Furthermore, board members often played a key role in the start-up phase of RM. Company C, Ardo and Company B, by contrast, indicated that their board's role in RM is rather limited as board members only receive reporting and give their approval. In the case of Company C, this is more than offset by the high degree of support from the CEO. Ardo and Company B, on the other hand, do not experience this assistance by the top and have less advanced RM systems and structures at their disposal. Based upon these findings, I can definitely conclude that the tone set at the top is decisive for the maturity level of a company's RM function. I will come back at this point when discussing the fourth research question.

When looking at the structure of the board, none of the interrogated companies have a separate risk committee. Alternatively, the risk role is delegated to the audit committee, except for Ardo and Raffinerie Tirlemontoise. Ardo's board as a whole is responsible for RM since there is no audit committee. Raffinerie Tirlemontoise also does not have an audit committee since this is installed at the group level, at Südzucker. Company A is the only company in this case study that ever had a separate risk committee at board level. But because of overlapping duties, the company decided to combine audit and risk responsibilities into one committee. Colruyt gave a similar explanation as it also referred to the overlap with the audit committee. Others stated that a separate risk committee would be too ambitious and/or that the benefits would not outweigh the costs. Overall, Belgian companies consider a separate risk committee at board level as unnecessary. In most cases, the audit committee oversees the whole risk process and reviews its effectiveness. The committee assists and advises the board in terms of RM, but the final responsibility rests with the board as a whole. A different division of the tasks can be found in the Colruyt case, where the audit committee deals with the financial risks while the board as a whole monitors the strategic risks.

### **5.3.2. Strategic risk management**

The literature study revealed the importance of SRM. The second research question investigates whether Belgian companies link RM with their business strategy. The data on this topic can be found in the last column of the matrix in appendix 12. Three of the eight companies were really aware of the added value of SRM and had already implemented appropriate systems. First of all, Proximus referred to SRM as its number one priority. The company has structured systems in place to respond to those risks that could have an impact on its strategic objectives. During the strategy process, questions are raised by the RM area. At this moment, the company is improving its annual survey to better identify its strategic risks. Other companies, however, argue that a survey does not suffice and that personal involvement on the field is essential to uncover strategic risks. Secondly, Colruyt's Coris programme is based on the company's strategy. Risks are being identified by closely examining the strategic objectives. Colruyt's risk register also has a special category devoted to strategic risks. Finally, the RM function of Company C pays a lot of attention to the risks and uncertainties associated with the recent strategic plan. The other companies are largely aware of the benefits of SRM, but they have not yet developed appropriate systems. Company D is currently examining how SRM could be implemented in the organisation. However, there is a lack of support from the ExCo and the board. Company A already has a lot of experience with RM as it was one of the first Belgian companies active in this area. Despite the fact that their strategy is developed in close collaboration with the RM department, there is still a lot of room for improvement in the area of SRM. Finally, Ardo and Company B are currently not working on SRM.

### **5.3.3. Internal risk reporting and information provision**

The information collected concerning the third research question on internal risk reporting is structured in a separate matrix in appendix 13. First of all, I examined how Belgian companies have organised their internal reporting lines. Six of the eight organisations have a similar structure. Their RM team and/or corporate risk manager report directly towards the executive management and the audit committee. The only difference visible is the designated contact person in the ExCo. Risk managers are in contact with either the CFO, CEO, COO or other C-suite level executives. This depends on who has been appointed as RM leader at the executive level. Besides the ExCo, the board is also provided with risk information through the audit committee. Most risk managers attend every audit meeting to give a presentation of the risks and their evolution in the past period. Once the information has reached the audit committee, this in its turn presents an even more summarised version to the board as a whole. All organisations gave the impression to be satisfied with their internal reporting practices. It allows their executive management and board to be aware of the key risks and properly

fulfil their risk oversight role. At Company C, however, the risk manager is only allowed to attend that part of the audit committee where he has to present the risks. This impedes him from gaining information from other sources. A similar practice is found in Company A, where the risk manager is not invited to board meetings, but always has to be stand-by to provide additional explanation if necessary. However, in contrast with Company C, this is a consequence of the company's very informal culture and there is no question of insufficient access to information. The only company that really derogates from this general reporting structure is Ardo, since it has no formal risk reporting line. Risks are only implicitly being discussed during Ardo's management and board meetings. The reporting line of Raffinerie Tirlemontoise is also deviating from the pattern. But this can be explained by the fact that its RM is largely in the hands of its parent company Südzucker.

Besides having appropriate reporting lines, organisations should also pay attention to the frequency and timing of the reporting. I can conclude that formal risk reporting mainly coincides with the timing of audit meetings. Except for Ardo and Raffinerie Tirlemontoise, every company's audit committee holds at least quarterly meetings. Depending on the actual events and results, they schedule additional sessions. Before every meeting, written reports are sent to the members of the audit committee. During the meeting risk managers give a short presentation of the risks and answer additional questions. As already mentioned, the audit committee then presents the information to the entire board. The provision of information to the executive committee generally occurs with the same frequency. Five companies mentioned that their formal reporting systems are supplemented with more frequent informal communication. Colruyt's risk manager, for example, repeatedly pointed at his easy access to and frequent information exchange with the top. Moreover, the executive and board level of this company are closely linked because of the strong family ties. Proximus also has a high degree of internal communication. Their risk director has weekly meetings and even more face-to-face contacts with members of the ExCo. A final example is Company A, which has a very open and accessible corporate culture with a lot of informal communication.

In terms of the content, multiple interviewees referred to the importance of not overwhelming the higher corporate levels with too detailed information. In accordance with the findings from the literature study, risks are often ranked based on their likelihood and impact on the business. Afterwards, only the key risks are presented to the executive and board level. The final number of submitted risks varies from company to company, going from three key risks to a top 20 of risks facing the firm. Colruyt and Company D stated that they also divide the risks into different categories. In this way, they can quickly retrieve and report the risks of a certain area. The audit committee usually receives a more detailed list of risks, because they have to oversee and evaluate the whole risk process.



In order to present the risks as clearly as possible, five companies make use of visual tools in their presentations. These tools are the ones that were mentioned in the literature study, but can also vary depending on what each company considers important. Multiple companies make use of risk matrices with two axes that indicate each risk's impact and likelihood. Moreover, risk scorecards provide more detailed information such as the current and previous status of the risk, risk owner, KRIs, mitigating actions, etc. Based on the documents that companies presented me during interviews, I can conclude that they usually apply colour codes to indicate the importance of a certain risk. Only three companies barely use one of these tools. Company A is aware of its backlog in this area. Ardo, on the other hand, relies on informal information exchange without visual elements. And finally, Raffinerie Tirlemontoise is aware of the existence of visual tools, but currently does not use them.

#### **5.3.4. Determinants**

In order to examine the determinants of RM, I used the summary table of the company characteristics in appendix 11. Moreover, I structured findings and quotes from the interviews relating to different determinants in a matrix in appendix 14.

##### *Firm size*

A lot of the findings of the literature study relating to firm size can be confirmed by this case study. Small businesses were not even included because I could distract from their corporate information that they barely give active consideration to RM. Based on the analysis of the companies involved, I found that the largest companies in terms of annual revenue (Colruyt, Proximus, Company A and Company D) are equipped with more mature RM practices than smaller firms. Colruyt, the largest company in this study, clearly has the most advanced ERM program. This was also confirmed by other companies who consider the Coris programme as an example for their own RM.

Large companies have specific functions in place to guide the risk process. Each of these four largest organisations has a RM team or department while smaller companies usually only have a single person dealing with RM. Smaller businesses sometimes delegate this role to an existing corporate position, such as the internal auditor at Company B. Previous studies mentioned that larger firms are more likely to appoint a CRO and install a separate risk committee in the board. However, this could not be confirmed as none of the interrogated companies appointed a CRO or risk committee. CROs and board risk committees are too advanced for Belgian companies. They mainly occur in much bigger U.S. organisations. Previous research also showed that the majority of organisations still prefer to delegate the risk responsibilities to the audit committee. This is also the case for most companies in this study, as they almost all have an audit committee that oversees the risk process.

When comparing the risk reporting practices of small and large companies, there were no remarkable differences. Almost all the companies, both small and large, are reporting on a quarterly basis to the top and thereby make use of visual tools and colour codes. Ardo is the only company that really deviates from the other companies in this study. Despite its large size, the company has no advanced RM programme nor formal reporting lines. This can be explained by the fact that the company reduces its risks in a different way, by means of long-term contracts and a geographical distribution of activities.

### *Type of industry*

It is needless to say that risks can vary widely depending on the range of activities of a company. Nevertheless, after comparing all the cases, I can conclude that the industry has no big impact on the design of the RM function. Most of the interviewed companies implement similar RM and internal reporting structures, regardless of their specific industry. This conclusion is also confirmed by the fact that multiple companies share best practices in RM, even across different sectors. Proximus' risk director mentioned that he compares his way of working to other organisations to learn and to find out where his company is standing in terms of RM. Moreover, Company A's risk manager does not believe that there are fundamental differences between sectors. He also mentioned that his company shares RM practices with members of BELRIM and FERMA. As a final example, Colruyt's risk manager mentioned that he gives lectures in other companies to describe the Coris programme. The literature study also mentioned the large difference between financial and non-financial companies. However, given their complexity and completely different RM approach, financial organisations were not included in this study. Therefore, I cannot comment on this assumption.

An important factor that is associated with the type of industry, is the level of regulation. This can have a strong influence as some sectors are subject to very strict legislations. On the one hand, four companies referred in this context to the GDPR, the new European law on data privacy and security. Non-compliance with this new regulation is one of the key risks for companies active in the telecommunications or IT industry. Company A and Proximus emphasised the importance of data security for their activities. Company B in its turn is developing formal structures and procedures to comply with the new regulation. Company D's risk department even considers a merger with the compliance department to create synergies and better focus on non-compliance risks. Colruyt, on the other hand, has a separate internal position devoted to the severe competition legislation.

### *Complexity*

Every company in this case study consists of multiple business units. RM is usually a corporate function that operates above the different departments. Therefore, the number of BUs is not considered to have an influence on the organisational structure for RM. In accordance with the findings relating to

the type of industry, the number of divisions only has an influence on the amount and type of risks, but not on the risk oversight structure.

Most of the interrogated companies are active in Belgium and some neighbouring countries. Therefore, they do not experience an impact of large cultural differences on their RM practices. One of the exceptions is Company A, as it operates in seven different countries worldwide. Its risk manager consequently referred to the impact of the ever-changing world, especially to the geopolitical situation. He stated that this increased people's awareness for RM and they now more often request his opinion. Company C and Raffinerie Tirlemontoise also have worldwide activities, but this does not significantly influence their RM function.

#### *Ownership type*

Five out of the eight companies in this case study are publicly traded. Four of them are the large organisations that were mentioned in the paragraph on firm size. Therefore, the conclusions regarding their risk oversight practices largely coincide. In accordance with the literature study, publicly traded companies have more advanced RM practices and reporting systems compared to private businesses. Listed companies are subject to the Belgian Code on Corporate Governance. They therefore have to clearly describe and annually assess their internal control and risk frameworks in their annual report. Moreover, listed companies have to set up a board level audit committee, which has to review the internal RM systems. Company B, for example, is the smallest company of the ones I interviewed, but due to its stock exchange listing, it also has to give active consideration to RM. Therefore, the risk role is fulfilled by its internal auditor and the audit committee oversees the whole risk process.

By way of contrast, Company C is a private company that does not have to comply with the Code on Corporate Governance. But given the size and the risky character of its industry, this company however has advanced systems and specific positions devoted to RM. Another remarkable finding in this context is that certain companies were already paying attention to RM before the introduction of the Code on Corporate Governance. Company A, for example, mentioned that it already had to comply with severe European laws in its sector even before the introduction of the Code on Corporate Governance. Moreover, the risk manager believes that the company's conversion of activities had more influence than the stock market listing. Colruyt, on the other hand, stated that the implementation of a RM programme occurred at the request of their CEO. The Code on Corporate Governance had little influence on this company since they were already compliant with all its guidelines. Overall, I can conclude that publicly listed companies have more mature RM systems and structures compared to private firms. However, this is not always a direct consequence of compliance with regulations for listed companies. In most cases, listed companies are of substantial size and are therefore very attentive to risks. This notwithstanding, exceptions are possible, where private companies also

implement risk programmes based on their size and/or sector. I believe that especially firm size and ownership type should be taken together when investigating RM practices.

As has been mentioned in the literature study, the concentration of ownership can also be a determining factor for risk oversight. Company D, for example, is for a major part held by a U.S. company. This last company has to comply with the U.S. SOX regulation and therefore obliged Company D to develop a risk framework. In this way, Company D became aware of the need for a formal RM approach. At Raffinerie Tirlemontoise, the RM function is completely controlled by its parent company Südzucker. Another example is Company B, where 14% of the shares are held by another Belgian firm. This latter company has a very mature RM programme in place and shares this knowledge with Company B. The Anglo-Saxon shareholders of Company C also have a substantial impact on the company's RM because of their high sensitivity for official certificates. Companies that are to a large extent controlled by the Belgian State, are not affected by this specific shareholder in terms of RM. Given these points, I can conclude that the concentration of ownership generally has a large influence on risk oversight.

Another specific category are the family businesses. Close family ties particularly have an influence on the applied risk approach and reporting practices. As stated by Colruyt's risk manager, doing business with your own money, changes the way you look at risks. Family businesses are usually more risk averse compared to other businesses. The other family business in this case study, Ardo, also has a high degree of risk aversion. Moreover, they do not have a proper distribution of the risk roles and there are more overlapping responsibilities due to the close family ties. When having a look at the risk reporting practices, both Colruyt and Ardo have a high degree of transparency and informal information exchange. Ardo's board members are highly aware of the key risks because of the frequent communication between family members, even out of business hours.

#### *Board characteristics*

The size of the board varied from 7 to 14 members. The number of independent members and non-executive directors is for most companies largely determined by the provisions of the Code on Corporate Governance. A study in the past found that larger boards are more likely to delegate the risk responsibilities to the board as a whole, instead of holding a board committee responsible. This could not be confirmed since the majority of the interrogated companies delegate the risk responsibilities to the audit committee and the entire board, regardless of the number of board members. Furthermore, I could not find any other significant relationship between the size of the board and risk oversight.

### *Other determinants*

According to me, another important determinant is the support from the top for RM. This topic has already been discussed in the literature study in 3.2.2. when discussing the role of the board in RM. It was already mentioned that the tone for RM has to be set at the top in order to reach the bottom of the company. Nevertheless, I could not find any study where this determinant was investigated. In this case study, however, it definitely emerged as an influencing factor. When comparing all the individual cases, I found more mature RM programmes and structures in organisations where the executive and board level attach considerable importance to RM. Company A's risk manager, for example, mentioned that he did not have to convince the higher corporate levels of the benefits of RM, since it was imposed from above. Therefore, the company does not need a CRO to increase the attention attached to RM. The same applies to Colruyt, whose risk manager also stated that a CRO position is unnecessary because he already receives enough resources and assistance from the executive and board level. He repeatedly referred to the support from the top as one of the key success factors of the Coris programme. At Company B, by contrast, there is no commitment from the board for RM. This company also has no RM structures in place and its risk programme is still in its early stages. This again indicates the importance of sufficient support from above. Moreover, the higher the level of commitment at the top, the more informal risk reporting and communication. This is closely related to the impact of the company culture. Both Colruyt and Company C mentioned that the internal culture has a significant influence on the maturity level of their RM system. In order for RM to be effective, company members need to be convinced of the benefits of RM and be attentive to the risks associated with their actions. As a consequence, it is important for the executive and board level to lead by example and provide adequate support in terms of RM.

The introduction of this master dissertation mentioned the ever-changing and complex world in which organisations are currently operating. This definitely has an influence on companies' RM function. The recent terrorist attacks (2016), for example, made people realize that unforeseen events can have dramatic consequences. Different interviewees stated that they are now confronted with questions from their colleagues relating to terrorism. The same applies to the geopolitical situation. Whereas a few years ago, globalization was a hot topic, countries are now closing their borders and promoting their internal products. Ardo's managing director referred in this regard to the risks facing the company related to the Brexit. Company A stated that the recent financial crises also led to an increase in instability. In order to be better prepared for similar situations, RM is strengthening its position. As a consequence, organisations are improving their risk procedures and implement adapted structures. I can conclude that such disruptive global events contribute to the increasing interest in RM.

A summary table of the impact of the determinants can be found in appendix 15.

### 5.3.5. Consequences of risk oversight

It is, of course, also important to have a look at the results of all the efforts in terms of RM. Therefore, this case study also focuses on the output side of the RM processes. In particular, I asked companies which impacts of RM they perceive on their business results. After analysing the data from the interviews, a general pattern was visible (see appendix 16). The majority of the interviewees admitted not having a clear understanding of the impact of RM on their corporate results. First of all, RM usually has a rather preventive character. Companies try to avoid or at least reduce risks as much as possible. For this reason, the results are often invisible. Secondly, none of the interrogated companies measure the precise benefits and costs of their risk mitigating actions. Different interviewees referred to this as *“a difficult exercise”*. Companies rather monitor the evolution of risks over time. Despite the fact that there are no actual figures available on the results of RM, six out of the eight interviewees almost literally referred to the positive consequences for their company. Company D, for example, discovered a lot of revenue leakage through its risk programme. Company A stated that their mature RM system often saves costs when they have to comply with new regulations. Other companies referred to the higher return for shareholders and improved credit rating because of their advanced RM systems.

In contrast to the unclear impact on the business results, I noticed an apparent influence of RM on the corporate risk culture. Six out of the eight interviewees were very enthusiastic about the change in their people’s mindset. They perceive a growing internal awareness for RM. Employees are becoming increasingly aware of the benefits of a more structured risk approach and they more often consider the risk implications of their actions and decisions. Whereas in the past Colruyt’s risk manager used to assess the risks associated with certain projects on his own initiative, he is now often consulted at the request of a subordinate. In addition, Company C’s risk manager stated: *“Colleagues are more likely to come to me and they appreciate my contribution”*.

Regarding the influence on the level of risk taking, I found contradictory information. The interviewee of Company B, on the one hand, stated that RM efforts sometimes have the opposite effect of an increase in risk aversion. The same applies to Raffinerie Tirlemontoise. However, in order to create added value, companies must dare to take certain risks. Colruyt’s risk manager, on the other hand, claimed that he perceives no real impact on the level of risk aversion, as it is rather a new way of dealing with the same risks. Other companies did not mention any consequences for their level of risk taking. Overall, I can say that for most companies, there is no heightened risk aversion.

## 6. Conclusion

### 6.1. General conclusions

The qualitative study contributed to the existing knowledge by investigating the risk oversight roles of the executive and board level in Belgian companies, as well as the associated determinants and consequences. I had the opportunity to conduct interviews with eight companies to collect a large amount of information. In this final conclusion, I will summarize the most important findings.

First of all, every interrogated company has its own risk oversight structure, tailored to its specific characteristics and needs. Nevertheless, I found some general similarities regarding their assignment of risk roles and responsibilities at executive and board level. The risk ownership is usually spread across the different departments, while a central risk department coordinates the whole risk process. This department either consists of different members or is solely composed of the corporate risk manager. Together with the executive committee, the risk department drafts proposals on the risk approach and the suitable risk programs and procedures. The board then has to take decisions based on the proposals. The audit committee often assists board members in this task and frequently evaluates the effectiveness of the risk approach. None of the interrogated companies have explicitly appointed a CRO nor created a separate risk committee at board level. These positions are considered to be too ambitious for Belgian companies. Moreover, they are unnecessary when there is already a high level of support and guidance from top management and board level. The role of CRO is often implicitly fulfilled by pre-existing corporate positions, such as the corporate risk manager, CEO or CFO.

The second research question focused on SRM, or the link between risk management and the corporate strategy. The study showed that the majority of the companies are already aware of the added value of SRM. Moreover, almost half of the interrogated organisations have advanced SRM systems in place. Their risk identification is closely coordinated with their strategic objectives. Nevertheless, in most companies, there is still room for improvement in terms of appropriate procedures for SRM. An important factor in this context is the support provided by the top, as this can accelerate the implementation process.

The study also examined the internal risk reporting and information provision. I can summarise by saying that most of the interrogated companies have a smooth supply of risk information to their executive and board level. The majority of the interviewees were also pleased with the current reporting practices. Most companies make use of similar reporting lines where the risk department has direct access to the executive management and the audit committee. The designated contact person varied from company to company. The audit committee in its turn presents the key risks to the

board of directors. This process usually happens on a quarterly basis and is supported by visual tools, such as risk matrices and scorecards. More than half of the companies stated that they have more frequent informal information exchange by means of face-to-face contacts and other personal communication tools. Nevertheless, there is still room for improvement for some companies where the information provision is limited to official reports. Moreover, a few companies do not yet take advantage of visual elements in their presentations.

Furthermore, this study identified the key determinants of risk oversight practices. First of all, I noticed a large difference between small and large companies as larger organisations usually have more advanced risk management programmes. Given their larger number of risks, they have special positions devoted to risk management. Small companies, by contrast, are less committed to risk management. Furthermore, the type of industry did not have a significant impact on how Belgian companies are organised in terms of risk oversight. Most companies in this study are even sharing best practices across sectoral boundaries. Nevertheless, the level of regulation, which is heavily depending on the type of industry, turned out to be an influencing factor. Organisations have to comply with severe regulations and this often results in the creation of specific functions and/or committees. Another important determining factor is the ownership type. Publicly listed firms are subject to the Belgian Code on Corporate Governance, which means that they have to give a detailed description of their risk management system in their annual report. Moreover, they are obliged to install an audit committee at board level. Private companies, by contrast, are free to determine their own risk approach. Nevertheless, when they are of substantial size, private firms often have risk oversight practices in place that are similar to listed companies. I found that, besides their main effects, firm size and ownership type have certain interaction effects. Special attention was also devoted to the concentration of ownership and family businesses as these two variables also have a decisive influence. Finally, organisational complexity and board characteristics do not affect the risk oversight practices.

Besides investigating the determinants that were mentioned in the literature study, the interviews also revealed two additional factors. First of all, the support from the top was repeatedly mentioned as one of the key success factors of risk oversight. The managerial and board level should lead by example in order to increase the internal awareness for risk management. Secondly, disruptive events in the rapidly changing environment of companies are also affecting their risk oversight practices.

Another meaningful contribution to the existing knowledge on risk oversight was the investigation of its consequences. I mainly found a significant impact on the corporate risk culture, as there is a fundamental change in people's mindset. Company staff more carefully consider the risks associated with their actions and they more often consult the risk experts.



## 6.2. Recommendations and limitations

One of the limitations of qualitative research is the small size of the sample. Therefore, the abovementioned conclusions cannot be generalised to the entire population of Belgian companies. Nevertheless, the individual cases were very informative and I found some interesting common patterns that can be further examined in the future. According to me, there are especially possibilities for additional investigation in the area of the determinants and consequences of risk oversight. This case study already exposed some interesting factors such as firm size, level of regulation, ownership type and support from the top. The significance of these determinants can be further examined in a quantitative study with a large sample of companies. In terms of the consequences of risk oversight, this study principally uncovered an apparent influence on the corporate risk culture as there is an increasing internal awareness for risk management. Regarding the level of risk taking, there was inconsistency between the different companies. Therefore, it would be worthwhile to conduct further research on this topic. The literature study already mentioned the possibility to investigate the volatility in companies' stock returns as an indication of their risk behaviour (Ellul&Yerramilli, 2013).

Furthermore, this study solely focused on non-financial companies. The literature study, however, clearly indicated that these companies significantly differ from financial services organisations. I therefore suggest to conduct a similar qualitative study in financial companies in order to identify the key differences. Another possibility is to carry out a large qualitative study including both financial and non-financial companies.

Despite these limitations, I believe that the reported conclusions provide clear insights into the current state of risk oversight at executive and board level in Belgian companies.

## REFERENCES

- Aksel, K. H. (2015). *Organizing a Financial Institution to Deliver Enterprise-Wide Risk Management*. Retrieved January 20, 2017, from [http://www.pwc.com.tr/en/assets/about/svcs/abas/frm/operationalrisk/articles/pwc\\_enterprisewiderisk.pdf](http://www.pwc.com.tr/en/assets/about/svcs/abas/frm/operationalrisk/articles/pwc_enterprisewiderisk.pdf)
- Ardo. (2014). *Ardo/Dujardin Foods Fusie Goedgekeurd*. Retrieved April 12, 2017, from <https://ardo.com/nl/actualiteit/food-service-solutions/2014/09/ardo-dujardin-foods-fusie-goedgekeurd>
- Atkinson, W. (2008). Board-Level Risk Committees. *Risk Management*, 55(6), 42-46.
- Ballou, B., Heitger, D. L., & Stoel, D. (2011). How Boards of Directors Perceive Risk Management Information. *Management Accounting Quarterly*, 12(4), 14-22.
- Beasley, M. S. & Frigo, M. L. (2007). Strategic Risk Management: Creating and Protecting Value. *Strategic Finance*, 25-33.
- Beasley, M., Branson, B., & Hancock, B. (2014). *Report on the Current State of Enterprise Risk Oversight: Opportunities to Strengthen Integration with Strategy*. North Carolina State University.
- Beasley, M., Branson, B., & Hancock, B. (2016). *Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities*. North Carolina State University.
- Belgian Risk Management Association. (2017). Retrieved January 20, 2017, from <http://www.belrim.com/members/>
- Berg, T., & Westgaard, S. (2012). *Risk Reporting to the Board of Directors: Field Study among Norwegian Banks and Power Companies*. Trondheim: Handelshoyskolen BI.
- Boyd, S. R., Moolman, J. A., & Nwosu, N. J. (2016). *Risk Reporting & Key Risk Indicators – A Case Study Analysis*. Retrieved January 29, 2017, from [https://erm.ncsu.edu/az/erm/i/chan/library/ERM\\_KRI\\_Case\\_Study\\_FINAL.pdf](https://erm.ncsu.edu/az/erm/i/chan/library/ERM_KRI_Case_Study_FINAL.pdf)
- Branson, B. (2015). *Reporting Key Risk Information to the Board of Directors: Top Risk Executives Share Their Practices*. North Carolina State University.
- Brodeur, A., Buehler, K., Patsalos-Fox, M., & Pergler, M. (2010). A board perspective on enterprise risk management. *McKinsey & Company*, (18), 1-15.

Bugalla, J., Kallman, J., Mandel, C., & Narvaez, K. (2012). Best Practice Risk Committees. *Corporate Board-Okemos*, 33(194), 6.

Carter, C. & Lorsch, J. W. (2002). *Back to the drawing board: Designing corporate boards for a complex world*. Boston: Harvard Business School Press.

Charan, R. (2009). *Owning Up: The 14 Questions Every Board Member Needs to Ask*. San Francisco: Josey Bass.

Colruyt Group. (2016). *Corporate Governance*. Retrieved April 23, 2017, from [https://www.colruytgroup.be/sites/default/files/financial/annualreports/pdf/page/669469\\_jr16\\_corporate\\_governance\\_eng\\_def\\_lr.pdf](https://www.colruytgroup.be/sites/default/files/financial/annualreports/pdf/page/669469_jr16_corporate_governance_eng_def_lr.pdf)

Commissie Corporate Governance. (2009). *Corporate Governance Code 2009*. Retrieved March 28, 2017, from <http://www.corporategovernancecommittee.be/sites/default/files/generated/files/page/corporategovernancecode2009.pdf>

COSO (2009). *Effective Enterprise Risk Oversight – The Role of the Board of Directors*. Retrieved January 29, 2017, from [https://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409\\_001.pdf](https://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf)

COSO (2013). *Enterprise Risk Management — Integrated Framework*. Retrieved October 23, 2016, from <http://www.coso.org>.

DeLoach, J. (2016). *Six Principles for Improving Board Risk Reporting*. Retrieved January 29, 2017, from <https://blog.nacdonline.org/2016/03/six-principles-for-improving-board-risk-reporting/>

Denis, D.K. (2001). Twenty-five years of corporate governance research... and counting. *Review of financial economics*, 10(3), 191 – 212.

Dickinson, G. (2001). Enterprise risk management: Its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance. Issues and Practice*, 26(3), 360-366.

Dionne, G. (2013). *Risk Management: History, Definition and Critique*. Montréal: Cirrelt.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 14(4), 532-550.

Ellul, A., & Yerramilli, V. (2013). Stronger risk controls, lower risk: Evidence from US bank holding companies. *The Journal of Finance*, 68(5), 1757-1803.

Ernst & Young (2013). *The Critical Role of the Board in Effective Risk Oversight*. Retrieved January 28, 2017 from [http://www.ey.com/Publication/vwLUAssets/The-critical-role-of-the-board-in-effective-risk-oversight/\\$FILE/The-critical-role-of-the-board-in-effective-risk-oversight.pdf](http://www.ey.com/Publication/vwLUAssets/The-critical-role-of-the-board-in-effective-risk-oversight/$FILE/The-critical-role-of-the-board-in-effective-risk-oversight.pdf)

European Commission (2016). *Directive 2010/73/EU of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading and 2004/109/EC on the harmonization of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market*. Retrieved November 12, 2016, from <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010L0073>

Fraser, J., & Simkins, B. (2009). *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*. Hoboken: Wiley.

Frigo, M.L., & Anderson, R.J. (2009). Strategic Risk Assessment: A first step for improving risk management and governance. *Strategic Finance*, 25-33.

Frigo, M. L., & Anderson, R. J. (2011). *Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance*. Retrieved November 2, 2016, from <http://wileyonlinelibrary.com>

Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, 4(3), 28-36.

Gall, M. D., Borg, W. R., & Gall, J. P. (1996). *Educational research: An introduction*. Longman Publishing.

Gupta, P. P., & Leech, T. J. (2014). Risk Oversight: Evolving Expectations for Boards. *EDPACS*, 49(3), 1-21.

Hambrick, D. C. (2007). Upper echelons theory: An update. *Academy of Management Review*, 32, 334-343.

Haubenstock, M. (1999). Organizing a Financial Institution to Deliver Enterprise-Wide Risk Management. *Journal of Lending and Credit Risk Management*, 1, 46-52.

Hilb, M. (2012). *New Corporate Governance: Successful Board Management Tools* (4<sup>th</sup> edition). St. Gallen: Springer.

Hung, H. (1998). A Typology of the Theories of the Roles of Governing Boards. *Corporate Governance*, 6(2), 101-111.

Ingle, C., & Van der Walt, N. (2008). Risk Management and Board Effectiveness. *International Studies of Management & Organization*, 38(3), 43-70.

- ICGN (2015). *Guidance on Corporate Risk Oversight*. Retrieved January 22, 2017, from [https://www.icgn.org/sites/default/files/ICGN%20Corp%20Risk%20Oversightweb\\_0.pdf](https://www.icgn.org/sites/default/files/ICGN%20Corp%20Risk%20Oversightweb_0.pdf)
- ISO (2009). *ISO 31 000 - Risk Management*. Retrieved November 15, 2016, from <http://www.iso.org/iso/home/standards/iso31000.htm>
- Ittner, C. D., & Keusch, T (2014). *Inside the Black Box: The Characteristics and Consequences of Board Risk Oversight*. University of Pennsylvania, Harvard Law School.
- Ittner, C. D., & Keusch, T. (2014). *The Determinants and Implications of Board of Director's Risk Oversight Practices*. University of Pennsylvania, Harvard Law School.
- Ittner, C. D., & Oyon, D. F. (2014). *The Internal Organization of Enterprise Risk Management*. University of Pennsylvania, University of Lausanne.
- Jablonowski, M. (2001). Thinking in Numbers. *Risk Management*, 30-35.
- Johanson, D. (2008). Corporate governance and board accounts: exploring a neglected interface between boards of directors and management. *Journal of Management and Governance*, 12(4) , 343 – 380.
- Kalia, V., & Müller, R. (2007). *Risk Management at Board Level: A Practical Guide for Board Members*. Berne: Haupt.
- KPMG (2010). *The Audit Committee Journey: Adapting to Uncertainty, Focusing on Transparency*. Retrieved November 11, 2016, from <https://home.kpmg.com/pt/en/home/insights/2016/06/audit-committee-institute.html>
- Kurland, O. M. (1994). Communicating Effectively with the Board Room. *Risk Management*, 116-120.
- Lam, J. (2001). The CRO is Here to Stay. *Risk Management*, 48(4), 16.
- Lam, J., & Kawamoto, B. M. (1997). Emergence of the Chief Risk Officer. *Risk Management*, 41(4), 30-34.
- Liebenberg, A. P., & Hoyt, R. E. (2003). The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officers. *Risk Management and Insurance Review*, 6(1), 37-52.
- McKinsey. (2010). *The Five Attributes of Enduring Family Businesses*. Retrieved March 16, 2017, from <http://www.mckinsey.com/business-functions/organization/our-insights/the-five-attributes-of-enduring-family-businesses>

- Miccolis, J., & Shah, S. (2000). *Enterprise Risk Management: An Analytical Approach*. Atlanta: Tilling-Hast-Towers Perrin.
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Thousand Oaks: Sage publications.
- Miller, K. (1992). A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies*, 23, 311-332.
- Mintzberg, H. (1989). *Mintzberg on management: Inside our strange world of organizations*. Singapore: Simon & Schuster.
- NACD (2009). *Risk Management and the Board of Directors*. Retrieved January 22, 2017, from <https://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=17421>
- NBN (2017). *Discover the Added Value of Risk Management Standards*. Retrieved January 10, 2017, from <https://www.nbn.be>
- OECD (2014), *Risk Management and Corporate Governance*. Retrieved November 2, 2016 from <http://dx.doi.org/10.1787/9789264208636-en>
- Olson, D. L., & Dash Wu, D. (2015). *Enterprise Risk Management*. Singapore: World Scientific Publishing.
- Overzicht aandelen. (2017). Retrieved January 10, 2017, from <http://www.aandelencheck.be/>
- Patton, M. Q. (2002). *Qualitative research and evaluation methods*. California EU: Sage Publications
- Pirson, M., & Turnbull, S. (2011). Corporate Governance, Risk Management, and the Financial Crisis: An Information Processing View. *Corporate Governance: An International Review*, 19(5), 459-470.
- Protiviti. (2010). *Board Risk Oversight: A Progress Report*. Protiviti.
- Proximus Group. (2016). *Consolidated Management Report 2016*. Retrieved April 10, 2017, from <https://www.proximus.com/sites/default/files/Documents/Investors/Reports/2016/Q4/ConsolidateMgtRept2016.pdf>
- Raber, R. W. (2003). The role of good corporate governance in overseeing risk. *Corporate Governance Advisor*, 11(2), 11-16.
- Raffinerie Tirlemontoise SA. (2015). *Rapport Annuel 2014/15*. Retrieved April 10, 2017, from [http://www.raffinerietirlemontoise.com/en/Who-we-are/News-Publications/2015/~/\\_media/CE37165EB98B4D90A4B1E93B76EC2F05.ashx](http://www.raffinerietirlemontoise.com/en/Who-we-are/News-Publications/2015/~/_media/CE37165EB98B4D90A4B1E93B76EC2F05.ashx)

Spencer, K., & Hyman, V. (2012). *Risk Management: Your Role as a Board Member*. Chicago: First Nonprofit Organization.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, 16(4), 640-661.

Südzucker. (2016). *Annual report 2015/16*. Retrieved May 1, 2017, from [http://ir2.flife.de/data/sudzucker/igb\\_html/index.php?bericht\\_id=1000006&lang=ENG](http://ir2.flife.de/data/sudzucker/igb_html/index.php?bericht_id=1000006&lang=ENG)

Thiessen, K., Hoyt, R. E., & Merkley, B. M. (2001). A Composite Sketch of a Chief Risk Officer. *The Conference Board of Canada, Canada*.

Tonello, M. (2012). *Should Your Board Have a Separate Risk Committee*. Retrieved February 22, 2017, <https://corpgov.law.harvard.edu/2012/02/12/should-your-board-have-a-separate-risk-committee/>

Tricker, R. I. (1994). *International corporate governance*. Singapore: Simon & Schuster.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, 5(2), 207-232.

Van den Broeck, H. & Buelens, M. (2012). *Essentials: Beslissen*. Gent: LannooCampus.

Van der Elst, C. (2013). *The Risk Management Duties of the Board of Directors*. Financial Law Institute Working Paper. Retrieved November 29, 2016, from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2267502](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2267502)

Wharton University (2011). *Ten Years After 9/11 – Risk Management in the Era of the Unthinkable*. Retrieved January 22, 2017, from <http://knowledge.wharton.upenn.edu/article/ten-years-after-911-risk-management-in-the-era-of-the-unthinkable/>

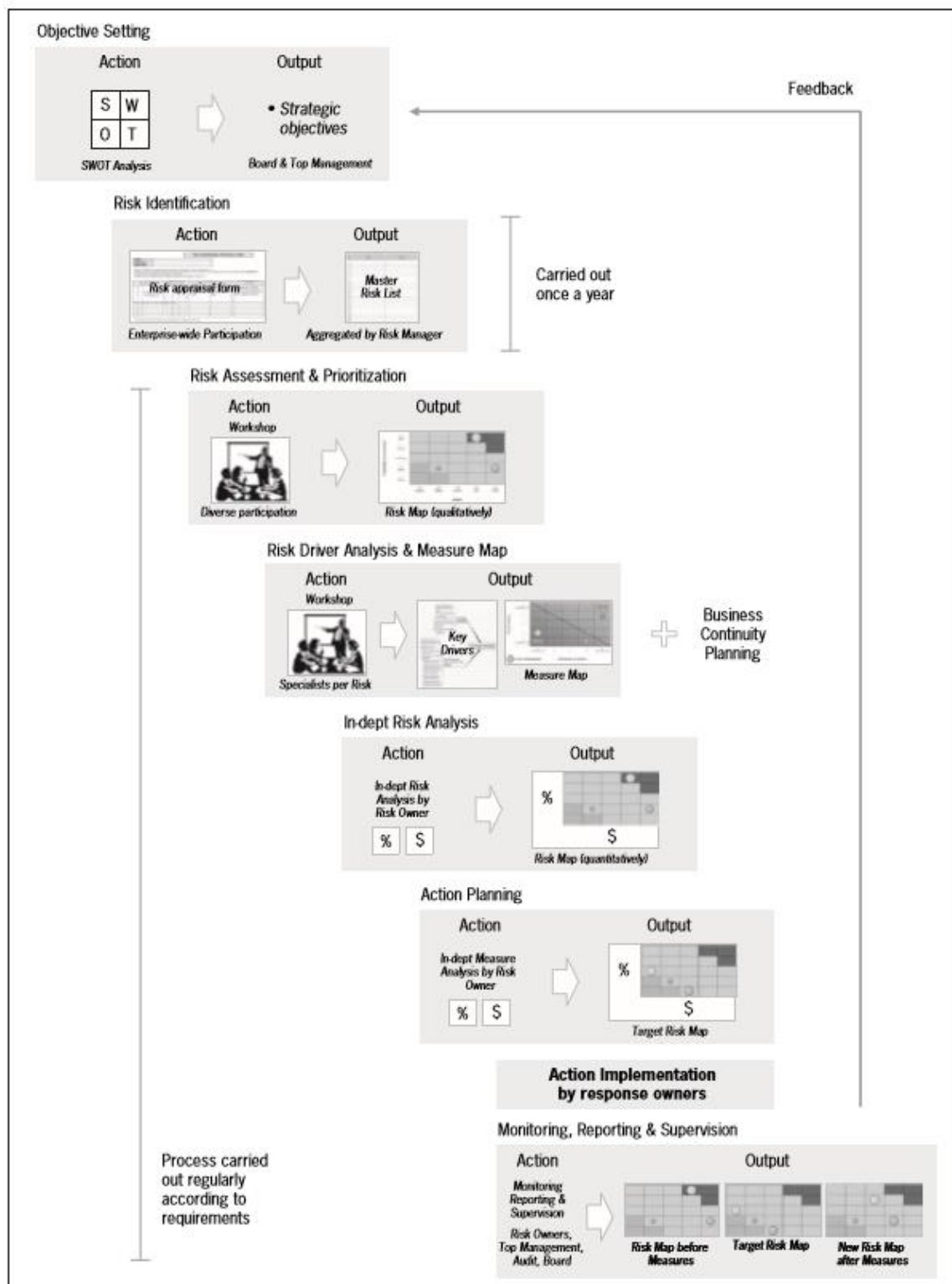
Williamson, D. (2007). The COSO ERM Framework: a Critique from Systems Theory of Management Control. *International Journal of Risk Assessment and Management*, 7(8), 1089-1119.

Yin, R. K. (2009). *Case study research: Design and methods*. Thousand Oaks: Sage publications.

Yin, R. K. (2014). *Case study research: Design and methods*. Thousand Oaks: Sage publications.

Zhang, P. (2010). Board information and strategic tasks performance. *Corporate Governance: An International Review*, 18(5), 473-487.

## Appendix 1: Risk management process

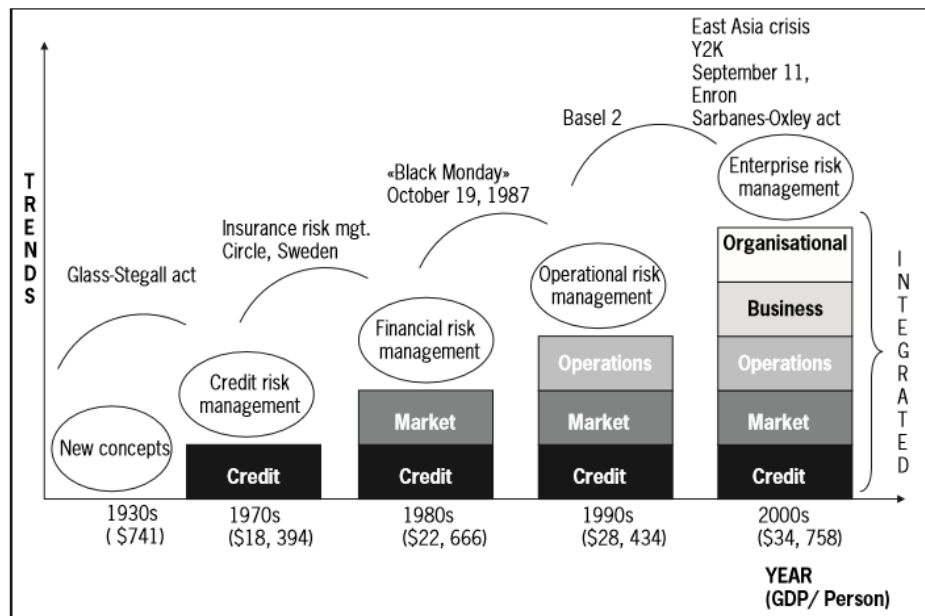


Source: Kalia&Müller, 2007.



## Appendix 2: The development of risk management

Despite the fact that organisations have always been confronted with risks and uncertainties, risk management itself is a relatively new area of interest (Dionne, 2013). The rise and development of risk management can be described in five stages as shown in the figure below:



The development of risk management. Source: Kalia&Müller, 2007.

### Stage 1: New concepts in the field (1930s)

The first notions of risk management already emerged in the 1930s. However, in the beginning, it concerned a bundle of measures without coherence nor systematic approach (Kalia&Müller, 2007).

### Stage 2: Credit risk management (1970s)

After World War II, different researchers started to investigate risk management. Modern risk management dates back to the period between 1955 and 1964. During the 1970s, risk management especially focused on insurance management (Dionne, 2013). The formerly unintegrated risk management activities became then more closely coordinated, which led to a more effective risk approach. Furthermore, the board started to recognise its final responsibility with regard to risk management (Kalia&Müller, 2007).

### Stage 3: Financial risk management (1980s)

Risk management developed into two directions during the 1980s: risk financing and risk control. Risk financing focused on financial derivatives, used to hedge a company's financial risks. Organisations also began to develop risk portfolios. Risk control, meanwhile, included a more comprehensive approach as managers began to realise the importance of a company-wide coordination of all risk activities (Dickinson, 2001; Kalia&Müller, 2007; Dionne, 2013).

#### *Stage 4: Operational risk management (1990s)*

Stage 4 occurred in the 1990s with the emergence of the first corporate functions devoted to risk management, such as the chief risk officer (CRO) who is held responsible for the company-wide supervision of risks. At the same time, the first international regulations regarding risk management appeared and led to a growing interest for this topic. In addition, integrated risk management emerged and there was increased attention to the governance of risk management (Dionne, 2013).

#### *Stage 5: Enterprise risk management (2000 onwards)*

Stage 5 occurred at the beginning of the 21<sup>st</sup> century as a result of different global unforeseen events such as the terrorist attacks on 9/11. Dramatic events of this scale emphasised that companies should think about the unthinkable and consider the major impacts of risks and volatility on their operational effectiveness and results (Wharton University, 2011). This all led to a new way of thinking about risks, called enterprise risk management (ERM). The main idea of this 360° approach on risk management is that organisations should deal with risks in a more integrated way instead of handling each risk separately. In order to be effective, the assessment and management of risks in different organisational functions and divisions must be closely coordinated (Kalia&Müller, 2007). ERM itself is then the foundation for another upcoming trend in risk management called strategic risk management (SRM). SRM requires organisations to consider the linkage between their business strategy and risk management approach (Frigo&Anderson, 2011).

## Appendix 3: Conceptual frameworks

Recently, different conceptual frameworks have been developed in order to assist organisations with their ERM implementation process. These frameworks give an overview of the most important principles and guidelines for effective ERM. They all recognise the importance of the leadership role of the board and senior management in the ERM implementation. While these frameworks and guidelines do not force organisations to apply ERM, they do increase the pressure for more structured and systematic risk management processes and reporting practices (Liebenberg&Hoyt, 2003; Frigo&Anderson, 2011; Ballou et al., 2011). The publication of these frameworks coincided with the development of the Sarbanes Oxley Act (SOX) for U.S. companies in 2002. Its main objective is to improve financial reporting and internal control in U.S. public companies. The law focuses on corporate governance, ethical behaviour, board composition and the independence of auditors (Kalia&Müller, 2007; Frigo&Anderson, 2011). Concerning risk management, the SOX provides various recommendations for the executive and board level. In order to proactively identify, manage and mitigate the risks, a risk management and compliance system must be established (Kalia&Müller, 2007; Ingley&Van Der Walt, 2008). Different Belgian companies are connected to or controlled by a U.S. company, and therefore the SOX might have an influence on their risk management systems. The next sections briefly describe the most important conceptual frameworks in the area of ERM.

### *Report of the NACD*

The National Association of Corporate Directors (NACD) was founded in 1977 and is an independent association of more than 17 000 directors from U.S. and overseas organisations of all ownership types. Its aim is to improve corporate governance by assisting directors in their decision-making process and risk oversight function. In 2009, the NACD released a report including 10 principles of effective risk oversight by the board. *Risk Governance: Balancing Risk and Reward*, contains both general business principles as well as specific principles focused on risk management. The content is similar to the COSO framework and emphasises the importance of internal communication and reporting on organisational risks (NACD, 2009; Ballou et al., 2011; Gupta&Leech, 2014).

### *Committee of Sponsoring Organizations Framework*

COSO was created in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an initiative of the private sector to expose the causal factors of fraud in financial reporting (COSO, 2013). Besides the disclosure of these causes, COSO assists companies and their boards in ERM by developing guidelines and presenting the first framework concerning ERM. The ERM – Integrated Framework aims to offer organisations a common reference frame for internal management and control. It dates back to 2002, but was updated in 2004 resulting in the COSO II of ERM Framework (Kalia&Müller, 2007; Frigo&Anderson, 2011 Berg&Westgaard, 2012).



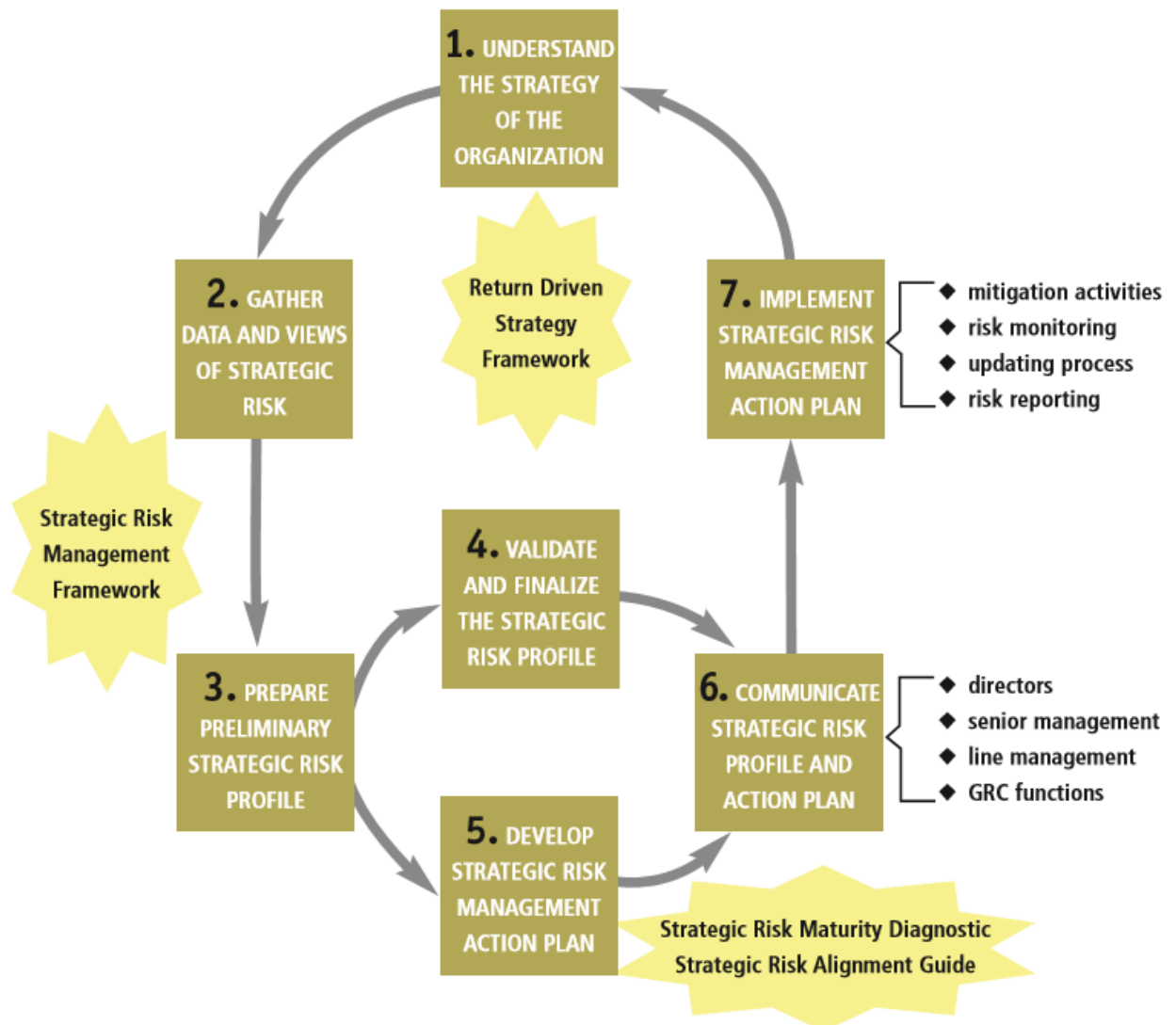
COSO framework. Source: COSO, 2013.

The figure above reveals COSO's integrated ERM framework of COSO. The horizontal axis shows the four key areas of organisational objectives according to COSO: strategic, operations, reporting and compliance. Within these four areas, senior management can cooperate with the board for better risk oversight (Ballou et al., 2011). The objectives apply to each of the organisational levels from the top to the bottom, namely entity-level, divisional level, business units level and subsidiary level. According to COSO, ERM consists of eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication and monitoring. The framework focuses on balancing the organisational risk appetite with the business strategy in order to provide added value to the stakeholders (Frigo&Anderson, 2011; Berg&Westgaard, 2012). The COSO framework has been criticised because it particularly focuses on internal corporate aspects without mentioning the external context in which an organisation operates. Opponents of the COSO framework claim that a company may never be considered as a closed system (Williamson, 2007).

### *ISO 31000*

More recently, the International Organisation for Standardization (ISO) also developed a standard to support companies with their ERM processes. *ISO 31000 (2009)* is a standard consisting of a framework, a process and multiple principles to assist organisations in the achievement of their predetermined targets and the identification of opportunities and threats. The provided guidelines can be applied in any type of organisation, regardless of the company's size or industry (ISO, 2009; Frigo&Anderson, 2011; Risk Management Event NBN, 2017).

## Appendix 4: Strategic risk assessment process



Source: Frigo&Anderson, 2009.

## Appendix 5: Information processing

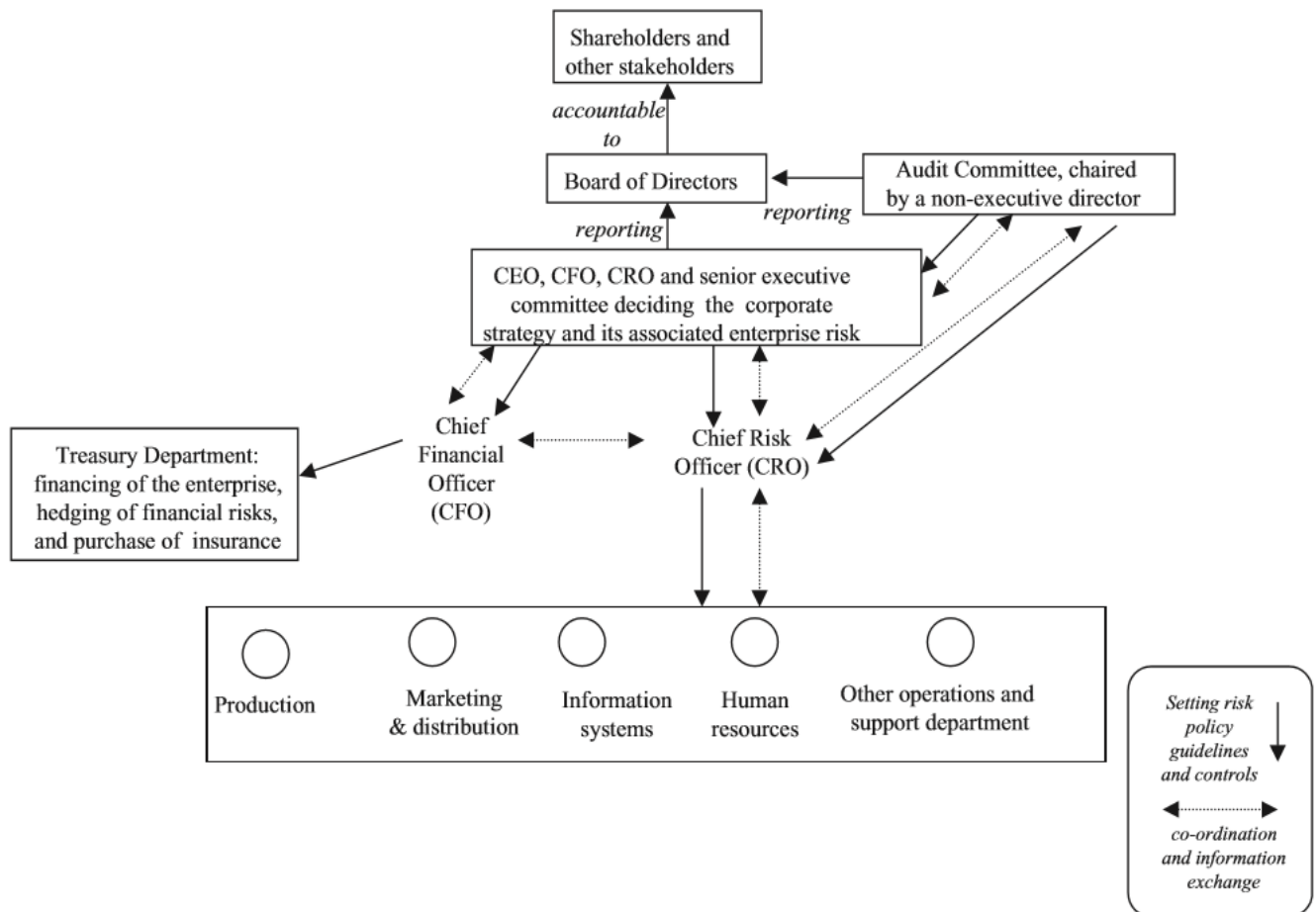
The resource-based view (RBV) of the firm focuses on how corporate resources can create a competitive advantage. The information that the board receives from its management team is often considered as an important resource. Recently, there has been an evolution in the RBV, suggesting that besides focusing on the static dimension of resources, there should also be enhanced attention to their dynamic dimension (Zhang, 2010).

Once the risk information has reached the board (static dimension), the effectiveness of risk oversight at board level is determined by how board members are processing the received information (dynamic dimension) (Zhang, 2010). During the financial crisis of 2007 – 2008, poor risk oversight at board level was caused by two specific problems in the board's information processing (Pirson&Turnbull, 2011). First of all, there was (and still is) the problem of asymmetric information, meaning that not all of the information known by the executive level is also presented to the board. Secondly, even if boards have access to relevant and complete risk information, they might fail in processing the information correctly. People are considered to be poor processors of information. They leap to conclusions without gathering and analysing the right amount and type of information (Tversky&Kahneman, 1973). Therefore, the board might be unable to correctly influence and guide the decision-making process of their management team (Zhang, 2010; Pirson&Turnbull, 2011; Gupta&Leech, 2014).

The greater the uncertainty of a certain task or decision, the more information that has to be processed by those involved to lead to a valuable decision or outcome. Uncertainty makes it difficult for decision-makers to plan everything in advance (Galbraith, 1974). Therefore, a higher degree of uncertainty generates more reporting and communication in a company. Given the extremely high degree of uncertainty in risk management, we can assume that a lot of information has to be processed by the board in order to achieve the desired outcomes. However, board members do not always have the right skills and capabilities to process the received information correctly (Pirson&Turnbull, 2011).








Even if boards only receive a limited amount of relevant risk related information, they might still be overwhelmed and undereducated to process the received data correctly (Carter&Lorsch, 2002). When confronted with an information overload, human beings try to exclude unfavourable information (Hambrick, 2007). Therefore, information regarding risks and uncertainties can be set aside. A lot of cognitive biases and heuristics also prevent people from being rational in the decision-making process. Both individual biases and group level phenomena prevent people from being rational. Groupthink, for example, means that group members prefer a consensus and a positive atmosphere to being honest and having different views and concerns (Van den Broeck&Buelens, 2012).

## Appendix 6: Risk reporting structure



Source: Dickinson, 2001.

## Appendix 7: Risk dashboard

Key Enterprise Risk	Risk Owner	Risk Status Q4 20XX (Prior Period)	Risk Status Q1 20XX (Current Period)	Risk Status Rationale	Key Risk Management Activities
<b>Resource Optimization</b> <b>Risk Definition</b> Inability to effectively allocate existing resources, and/ or secure additional qualified resources, to enable IH to optimize business activities (operational and strategic)	JR			-Current resource capacity sufficient to execute current portfolio -Governance structure in place to manage prioritization of work -ERP Redesign implemented -Etc.	-Prioritization of strategic initiatives to set groundwork for resource optimization -Implemented ERP -Etc.
<b>Medical Care Management</b> <b>Risk Definition</b> Inability to maintain medical costs within a range that is consistent with forecasted patterns, optimizes competitive position, and achieves target	TF			-"Partnerships and Alignments" initiatives are on track -"Medical Expense Management" strategies in development, targets set; new initiatives underway to identify additional opportunities -Risk management effectiveness is also dependent upon constituent engagement (members, providers and physicians) -Etc.	-Development of Medical Management Annual Plan for 20XX -Medical Management initiatives underway to identify new opportunities -Etc.
<b>Risk Status Key:</b>  <div>  <b>High:</b> risk management activities have not resulted in demonstrated improvement in the inherent risk exposure                     </div> <div>  <b>Medium:</b> risk management activities have begun to demonstrate improvement in the                     </div> <div>  <b>Low:</b> risk management activities have resulted in demonstrated improvement to adequately address or exceed inherent risk                     </div>					

Source: Branson, 2015.



## Appendix 8: List of companies in the target group

Naam Bedrijf	Sector	Symbol
AB InBev	Consumenten goederen	ABI
Ablynx	Gezondheidszorg	ABLX
Agfa-Gevaert	Industrie	AGFB
arGEN-X	Farmacie	ARGX
Barco	Industrie	BAR
Bekaert	Industrie	BEKB
Biocartis	Farmacie	BCART
Bone Therapeutics	Farmacie	BOTHE
Bpost	Transport & logistiek	BPOST
Celyad	Gezondheidszorg	CYAD
CFE	Industrie	CFEB
Colruyt	Consumenten diensten	COLR
D'leteren	Consumenten goederen	DIE
Daleny	Technologie	NYS
Deceuninck	Industrie	DECB
Econocom	Technologie	ECONB
Elia System Operator	Nutsbedrijven	ELI
Engie	Nutsbedrijven	ENGI
Euronav	Industrie	EURN
EVS Broadcast Equipment	Industrie	EVS
Exmar	Industrie	EXM
Fluxys Belgium	Olie & Gas	FLUX
Global Graphics	Technologie	GLOG
Greenyard Foods	Consumenten goederen	GRYFO
IBA	Gezondheidszorg	IBAB
Jensen Group	Industrie	JEN
Kinopolis Group	Consumenten diensten	KIN
Lotus Bakeries	Consumenten goederen	LOTB
MDxHealth	Gezondheidszorg	MDXH
Melexis	Technologie	MELE

Mithra Pharmaceuticals	Farmacie	MITRA
Nyrstar	Basismaterialen	NYR
Ontex Group	Consumenten goederen	ONTEX
Option	Technologie	OPTI
Orange Belgium	Telecommunicatie	OBEL
Picanol	Industrie	PIC
Proximus	Telecommunicatie	PROX
RealDolmen	Technologie	REA
Recticel	Basismaterialen	REC
Resilux	Industrie	RES
Retail Estates	Vastgoed	RET
Roularta Media Group	Consumenten diensten	ROU
RTL Group	Consumenten diensten	RTL
Saptec	Consumenten goederen	SAP
Sioen Industries	Industrie	SIOE
Sipef	Consumenten goederen	SIP
Smartphoto Group	Technologie	SMAR
Solvay	Basismaterialen	SOLB
Telenet Group	Consumenten diensten	TNET
Ter Beke	Consumenten goederen	TERB
Tessenderlo Group	Basismaterialen	TESB
ThromboGenics	Gezondheidszorg	THR
TiGenix	Gezondheidszorg	TIG
UCB	Gezondheidszorg	UCB
Umicore	Basismaterialen	UMI
Van de Velde	Consumenten goederen	VAN
Vastned Retail Belgium	Vastgoed	VASTB
Viohalco	Industrie	VIO
Wereldhave Belgium	Vastgoed	WEHB
Xior Student Housing	Vastgoed	XIOR
Zetes Industries	Technologie	ZTS

Source: <http://aandelencheck.be>, 2017.

## Appendix 9: Questionnaire – Dutch version

1. Sinds wanneer en in welke mate heeft uw bedrijf bewust aandacht voor **risicobeheer**?
  - a. Hebben er zich binnen uw bedrijf de afgelopen 5 jaar opmerkelijke veranderingen voorgedaan op vlak van risicobeheer en hoe dit georganiseerd is?
  - b. Wat waren eventuele aanleidingen voor de verhoogde aandacht voor risicobeheer?
2. Welke **formele rollen** werden er binnen uw bedrijf benoemd op niveau van het uitvoerend management en de board in het kader van risicobeheer?
  - a. Wat is de achterliggende motivatie om voor deze structuur te kiezen?
3. Is er op het niveau van het top management een **chief risk officer (CRO)** aangesteld als eindverantwoordelijke voor het risicobeheer?
  - a. Wat zijn de taken van de CRO?
  - b. Waar precies in het organigram van de organisatie kan de CRO gesitueerd worden?
  - c. Hoe verloopt de interactie tussen de CRO en andere leden van de risk management functie?
  - d. Indien er geen CRO werd benoemd, is er een andere senior executive aangesteld als **eindverantwoordelijke** voor risicobeheer op management niveau? Zo ja, welke taken vervult deze persoon? En is er bewust voor gekozen om geen CRO aan te stellen?
4. Is er een apart **risicocomité** of een aparte **risico afdeling** op het management niveau?
  - a. Indien JA, wie maakt deel uit van dit comité en welke taken worden door dit comité vervuld?
5. Wat is de rol van de **raad van bestuur** op vlak van risicobeheer van de organisatie?
  - a. Heeft de raad van bestuur op vlak van risicobeheer een puur toezichthoudende, controlerende rol of heeft ze een grote mate van inspraak in de manier waarop aan risicobeheer wordt gedaan binnen het bedrijf? In welke mate is de raad van bestuur actief betrokken bij het risicobeheer van de organisatie?
6. Hoe vertaalt dit zich in de **structuur** van de raad van bestuur? Is deze als geheel verantwoordelijk voor risicobeheer of zijn er aparte organen ontwikkeld die zich hiermee bezighouden?
7. Werd er binnen de raad van bestuur een apart **risico comité** aangesteld?
  - a. Wat is de achterliggende reden om een dergelijk comité aan te stellen?
  - b. Wat zijn de precieze taken van dit comité?
  - c. Wie maakt deel uit van dit comité? (afh. of onaf. leden, welke achtergrond, ...)
  - d. Hoe verloopt de samenwerking van dit comité met andere leden van de RvB?
  - e. Indien men geen afzonderlijk comité heeft opgericht, heeft men dit in het verleden ooit overwogen?
8. In welke mate is het **auditcomité** binnen de raad van bestuur betrokken in risicobeheer?
  - a. Indien het auditcomité verantwoordelijk is voor risicobeheer op niveau van de RvB, blijft de raad van bestuur als geheel dan ook nog verantwoordelijk voor deze functie?

9. Wat is de **strategische rol van de raad van bestuur**?
- a. Indien de raad van bestuur een duidelijke strategische rol vervult: Hoeveel aandacht is er voor risico's, bedreigingen vanuit de omgeving, opportuniteiten? Hoe wordt dit in het strategie proces opgenomen?
10. Hoe verloopt de risico **rapportering** en **informatievoorziening** op niveau van het top management en de raad van bestuur?
- a. Welke meetings er op het top management niveau georganiseerd omtrent risicobeheer? Hoe vaak worden deze meetings ingepland? Welke risico's worden hier besproken?
  - b. Rapporteert de *CRO of een andere eindverantwoordelijke voor risicobeheer* rechtstreeks aan de RvB/CEO/CFO/... ?
  - c. Kan u mij iets meer vertellen over de precieze *inhoud* van de rapportering tussen top management en board niveau?
  - d. Hoe verloopt deze rapportering? Schriftelijk/mondeling/beide?
  - e. Worden er *visuele elementen* gebruikt om de communicatie te ondersteunen? (risk map, risk scorecard, ...)
  - f. Hoe *frequent* en *wanneer* wordt er aan de RvB gerapporteerd omtrent risico's? Gebeurt de risico rapportering op vooraf bepaalde data of naar aanleiding van bepaalde belangrijke gebeurtenissen?
11. Zijn er bepaalde **variabelen** die volgens u een impact hebben op de manier waarop risicobeheer georganiseerd is binnen het bedrijf?
12. Wordt de risk management functie van het bedrijf regelmatig **geëvalueerd**? Hoe en door wie wordt de effectiviteit beoordeeld?
13. Welke **impact** heeft risk oversight (rol van de RvB en top management op vlak van risicobeheer) op de werking van de organisatie?
- a. Zijn er gevolgen voor de algemene resultaten van de organisatie?
  - b. Is er een impact op het risicogedrag/risicofilosofie van het bedrijf?
14. Bent u **tevreden** met de huidige werking van de risk management functie en de interne informatievoorziening omtrent risico's?
15. Hoe ziet u de risk management functie **evolueren** in de toekomst?

## Appendix 10: Questionnaire – English version

1. Since when and to which degree has the firm consciously given attention to **risk management**?
  - a. Have there been any significant changes in the past 5 years in the company's risk management and the way it is organised?
  - b. What were the potential triggers for the increased attention to risk management?
2. Which **formal roles** have been appointed in the company at the executive and board level in the context of risk management?
  - a. What is the underlying motivation to opt for this structure?
3. Is there a **chief risk officer (CRO)** who has the ultimate responsibility for the firm's risk management at the executive level?
  - a. What are the duties of the CRO?
  - b. Where exactly in the organisation chart can the CRO be situated?
  - c. How is the interaction between the CRO and other members of the risk management function?
  - d. If there is no CRO appointed, has the final responsibility for the risk management function been delegated to another person? If so, which tasks does he/she have to perform?
  - e. If there is no CRO appointed, was this a deliberate decision?
4. Is there a separate **risk committee** or separate **risk department** at the executive level?
  - a. If yes, who is included and which tasks are carried out by this committee?
5. What is the role of the **board of directors** in terms of the company's risk management?
  - a. Does the board rather fulfil a supervisory, controlling role or does it have a high level of control relating to the company's risk management? To what extent is the board actively involved in the firm's risk management?
6. How is this reflected in the **structure of the board**? Is the board as a whole responsible or are there separate bodies at board level that deal with risk management?
7. Is there a separate **risk committee** at board level?
  - a. What is the underlying motivation to appoint such a committee?
  - b. What are the precise duties of this committee?
  - c. Who is part of this committee? (dep. or indep. members, background, ...)
  - d. How is the cooperation between this committee and the other members of the board?
  - e. In the event of lack of a risk committee, has the company ever considered the appointment of such a committee?
  - f. Are there any specific reasons why the company decided not to appoint a separate risk committee at board level?
8. To what extent is the **audit committee** at board level involved in the firm's risk management?
  - a. If the audit committee is responsible for risk management, is the board as a whole still responsible for this issue?

9. What is the **strategic role of the board of directors** in the company?
- If the board has a clearly defined strategic role: How much attention does it pay to risks, threats in the surroundings and opportunities? How is this incorporated into the general strategic process?
10. How is **risk reporting and information provision** organised at executive and board level?
- Is risk management being discussed during meetings at top management level? How often are these meetings scheduled? Which risks are mentioned during these meetings?
  - Does the *CRO or another responsible* for risk management directly reports towards the board/CEO/CFO?
  - What is the precise *content* of the reporting between top management and board level?
  - How does the reporting takes place? Written/verbal/both?
  - Is the communication supported by *visual tools*? (risk map, risk scorecard, ...)
  - How *frequently* and *when* are the risks reported to the board? Does this happen on predetermined dates or rather in response to certain important events?
11. Are there according to you any **determinants** that influence the way risk management is organised in the company?
12. Is the company's risk management function often **evaluated**? Who determines the effectiveness and how does this happen?
13. What are the **consequences** of risk management/oversight for the company?
- Is there an impact on the general results?
  - Is there an influence on the company's risk behaviour/risk philosophy?
14. Are you **satisfied** with the internal risk management function and the information provision on risks?
15. How do you see the **future** of the company's risk management function?

## Appendix 11: Company characteristics

Company/ Characteristics	Firm Size (annual revenue and # of employees)	Industry	Complexity (# of BUs and geographic scope)	Ownership Type	Board Characteristics
<b>Colruyt</b>	- €9.18 billion - 29 683 empl.	retail & wholesale	- active in different sectors (food and non-food) - geo.: BEL + NLD + LUX + FRA	- publicly traded on BEL20 - Colruyt family: 51.88% of shares - remainder: held by the free float	- 9 members (6 family members) - 2 executive, 7 non-executive - 2 independent
<b>Proximus</b>	- €5.87 billion - ± 14 000 empl.	telecommunications	- 3 operational segments: consumer, enterprise and wholesale - geo.: BEL (+ NLD + LUX)	- publicly traded on BEL20 - Belgian state: 53.5% + 1 share - remainder: company itself, retail investors & internat. institutional shareholders	- 14 members - 7 appointed by the Belgian State - 7 independent
<b>Raffinerie Tirlemontoise</b>	- €530 million - ± 600 people	sugar production	- 4 BUs: sugar, Orafti, Surafti and PPE - geo.: active worldwide	- private - 100% controlled by the German food concern Südzucker	- 9 members: delegates of parent company Südzucker
<b>Ardo</b>	- €868 million - ± 3800 empl.	frozen food	- functional structure, no separate BUs	- private - family owned	- 10 members - 7 family members + 3 independent
<b>Company A</b>	- > €2.5 billion - > 10 000 empl.	digital imaging & information technology	- 3 BUs with own strategy, markets and customers - geo.: 7 countries	- publicly traded - internat. institutions and mutual funds	- 7 members - 4 independent
<b>Company B</b>	- > €230 million - ± 1000 empl.	information technology	- 3 key divisions - geo.: BEL + NLD + LUX	- publicly traded - public investors (> 50%) - large Belgian company (14%) - remainder: institutional shareholders	- 8 members - 7 non-executive + executive chairman - 5 independent
<b>Company C</b>	- €497 million - directly: 780 empl. - indirectly: 60 000 empl.	aviation industry	- 2 key segments	- Belgian State (25%) - private investors (75%)	- 11 members - CEO, chairman, 6 members designated by private investors and 3 appointed by the Belgian State
<b>Company D</b>	- €2.43 billion - ± 3300 empl.	telecommunications	- 3 BUs: private, B2B sales & role sale function - geo.: BEL (+ LUX)	- publicly traded on BEL20 - U.S. company: more than 50% of the shares - public: 33.29% - remainder: employees & other investors	- 10 members: CEO + 9 non-executive - 3 independent - large influence of the majority shareholder

## Appendix 12: RQ1 and RQ2 - Risk oversight structure and SRM

Company/ Topics	RM Department	Risk Role of the Ex. Level	Risk Responsibility in the ExCo	Risk Role of the BoD	Board Level Risk Committee	SRM
<b>Colruyt</b>	<ul style="list-style-type: none"> <li>- decentralised: every domain has to identify and manage its own risks</li> <li>- assistance from the RM team: corporate function (7 members)</li> <li>- combined with internal audit</li> </ul>	<ul style="list-style-type: none"> <li>- members of the ExCo are actively dealing with RM</li> <li>- CEO is the trigger for the risk programme</li> <li>- develop the risk approach in collaboration with the RM team</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- corporate risk manager can be regarded as the firm's CRO</li> <li>- no need for a CRO because of the high level of support from the top</li> </ul>	<ul style="list-style-type: none"> <li>- board places great importance on RM</li> <li>- wanted to increase the professionalism of RM</li> <li>- appointed a risk manager and asked for a risk programme</li> <li>- involved in the risk approach</li> </ul>	<ul style="list-style-type: none"> <li>- no separate risk committee: would overlap with audit committee</li> <li>- AC: financial risks</li> <li>- board as a whole: strategic risks</li> </ul>	<ul style="list-style-type: none"> <li>- Coris programme is based on the strategy</li> <li>- risks are identified in the context of the strategy</li> <li>- strategic risks as category in risk universe</li> </ul>
<b>Proximus</b>	<ul style="list-style-type: none"> <li>- RM department combined with internal audit</li> </ul>	<ul style="list-style-type: none"> <li>- determine the firm's risk appetite</li> <li>- oversee the key risks</li> <li>- discuss the risk approach in accordance with the strategy</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- RM and Compliance Committee: CCAO, CFO and CSO</li> <li>- director of ARC can be regarded as the firm's CRO: just below the executive level</li> <li>- no need for a CRO because of the direct reporting line to the ExCo</li> </ul>	<ul style="list-style-type: none"> <li>- "RM is very important for the board"</li> <li>- fully aware of the risks</li> <li>- assess the effectiveness of RM</li> </ul>	<ul style="list-style-type: none"> <li>- no separate risk committee: benefits would not outweigh the costs</li> <li>- role fulfilled by the AC and compliance committee: assists and advises the board</li> </ul>	<ul style="list-style-type: none"> <li>- ERM framework to respond to risks that could affect the strategy</li> <li>- "SRM is the nr.1 priority of this org."</li> <li>- "Risk assessment and evaluation takes place as an integral part of the annual strategic planning cycle".</li> <li>- survey to identify strategic risks</li> </ul>
<b>Raffinerie Tirlémontoise</b>	<ul style="list-style-type: none"> <li>- decentralised: different plants identify their own risks</li> <li>- director of the legal department is the final responsible for RM</li> <li>- no RM department</li> <li>- RM is group function: controlled by parent company, Südzucker</li> </ul>	<ul style="list-style-type: none"> <li>- director of legal department gathers and analyses risk information</li> <li>- "The strategy, guidelines and procedures for RM are now completely determined by our parent company"</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- final responsible: director legal department</li> <li>- no need for CRO because RM is controlled by the group</li> <li>- the group has a separate risk committee</li> </ul>	<ul style="list-style-type: none"> <li>- limited role</li> <li>- board members are representatives of the Südzucker</li> <li>- board: RM is very important</li> </ul>	<ul style="list-style-type: none"> <li>- no separate risk committee</li> <li>- role fulfilled by Südzucker's board: separate risk committee</li> <li>- no AC</li> </ul>	<ul style="list-style-type: none"> <li>- "In my view ERM is a hot topic"</li> <li>- "RM has evolved from pure operational ... to the assessment of risks of investments, new products etc."</li> <li>- increasing attention to strategic risks</li> <li>- no risk register or formal SRM</li> </ul>
<b>Ardo</b>	<ul style="list-style-type: none"> <li>- no separate risk department or elaborated risk approach: "That would be too formal for our company"</li> <li>- risks are implicitly considered as part of the business operations</li> <li>- every department has to assess and manage its own risks</li> <li>- some internal habits and procedures to guide decision-makers in RM</li> </ul>	<ul style="list-style-type: none"> <li>- receive reporting</li> <li>- being aware of the key risks</li> <li>- take risks into account when determining the strategy, investments and budgets</li> <li>- decide on contract terms and mitigating actions</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- no risk committee, the ExCo as a whole is responsible for the firm's risks</li> </ul>	<ul style="list-style-type: none"> <li>- overlap with the executive level because of the close family ties</li> <li>- has to come to agreements with the ExCo on risk strategies</li> </ul>	<ul style="list-style-type: none"> <li>- no risk committee</li> <li>- no AC</li> <li>- board as a whole responsible for RM</li> </ul>	<ul style="list-style-type: none"> <li>- "No, every department has to determine its own risks. This is not directly established based on the strategy of the firm"</li> <li>- no SRM</li> <li>- key risks are only implicitly related to the business strategy</li> </ul>



Company/ Topics	RM Department	Risk Role of the Ex. Level	Risk Responsibility in the ExCo	Risk Role of the BoD	Board Level Risk Committee	SRM
<b>Company A</b>	<ul style="list-style-type: none"> <li>- corporate risk manager is part of the company's small corporate management team</li> <li>- risk manager: responsible for RM and insurance management</li> </ul>	<ul style="list-style-type: none"> <li>- RM was imposed by the ExCo and the board</li> <li>- most active role in the firm's RM</li> <li>- identifies and assesses risks</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- CFO: the final resp. for RM</li> <li>- different executive committees responsible for quality, security, business continuity etc.: they all deal with risks in their own area</li> <li>- no need for a CRO because of high level of support from the top and direct reporting lines</li> </ul>	<ul style="list-style-type: none"> <li>- a lot of support for RM</li> <li>- <i>"coach", "partner"</i></li> <li>- a very active role in the firm, also in the context of RM</li> <li>- initial demand for RM came from the board</li> <li>- determine risk appetite</li> <li>- evaluate RM function</li> </ul>	<ul style="list-style-type: none"> <li>- risk committee and AC merged into one committee: AC: internal audit and RM works together (<i>"good and bad"</i>)</li> </ul>	<ul style="list-style-type: none"> <li>- board develops strategy in close collaboration with RM function</li> <li>- <i>"A risk manager has to support the global strategy of the company"</i></li> <li>- still room for improvement</li> </ul>
<b>Company B</b>	<ul style="list-style-type: none"> <li>- no independent RM department</li> <li>- RM is a responsibility of the internal auditor and the operational management</li> </ul>	<ul style="list-style-type: none"> <li>- final resp. for RM rests with the ExCo and the board</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- no risk committee in the ExCo</li> <li>- CFO: indirectly involved in RM</li> </ul>	<ul style="list-style-type: none"> <li>- limited role in RM</li> <li>- rather <i>"supervisory, controlling"</i></li> <li>- supervision of internal control and risk framework</li> <li>- determine risk appetite</li> </ul>	<ul style="list-style-type: none"> <li>- AC: oversee the RM process and advise the board + risk assessment</li> <li>- the secretary general can be seen as <i>"the point of contact for RM"</i></li> </ul>	<ul style="list-style-type: none"> <li>- limited attention to risks during the strategy process</li> <li>- still a lot of room for improvement</li> </ul>
<b>Company C</b>	<ul style="list-style-type: none"> <li>- RM department: corporate risk manager</li> <li>- monitor the risks that transcend the departments</li> <li>- combined with insurance management</li> </ul>	<ul style="list-style-type: none"> <li>- CEO created the RM department</li> <li>- <i>"Everything stands or falls with the directorate"</i></li> <li>- proposals on the firm's risk approach and its risk appetite</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- <i>"You could say that our CEO is the CRO"</i></li> <li>- CEO delegated RM to CFO and he delegated it to the risk manager</li> <li>- no need for a CRO</li> </ul>	<ul style="list-style-type: none"> <li>- <i>"The impact of the board is extremely limited"</i></li> <li>- <i>"completely pointless element"</i></li> <li>- receive reporting</li> <li>- give approval</li> </ul>	<ul style="list-style-type: none"> <li>- no separate risk committee</li> <li>- role fulfilled by the AC</li> <li>- AC: only receives reporting</li> </ul>	<ul style="list-style-type: none"> <li>- focus on strategic risks</li> <li>- 'Strategic Vision 2040': risks associated with this plan have been identified</li> </ul>
<b>Company D</b>	<ul style="list-style-type: none"> <li>- decentralised: ownership is spread across different functional areas</li> <li>- RM department: central oversight function (12 members): overview &amp; alignment</li> <li>- <i>"Make sure that different risk areas speak the same language"</i></li> <li>- indicate risk owners, recommend actions</li> <li>- consider a consolidation with the compliance department</li> </ul>	<ul style="list-style-type: none"> <li>- receive reporting</li> <li>- risk manager: wants more support from the top</li> </ul>	<ul style="list-style-type: none"> <li>- no CRO appointed in the ExCo</li> <li>- CFO: final resp. for RM</li> <li>- CRO would help to increase the attention to RM from the top: <i>"as member of the ExCo, he would have a greater participation and draw more attention to RM"</i></li> </ul>	<ul style="list-style-type: none"> <li>- verify management's actions</li> <li>- receive reporting</li> <li>- determine the risk appetite and profile</li> </ul>	<ul style="list-style-type: none"> <li>- no separate risk committee: <i>"over-ambitious for the company"</i></li> <li>- role fulfilled by the AC: assists and advises the board on RM + annual review of RM systems and procedures</li> <li>- final resp. remains with the board as a whole</li> </ul>	<ul style="list-style-type: none"> <li>- no formal system</li> <li>- ERM exercise to respond to the external demand for more attention to strategic risks</li> <li>- ExCo &amp; board prefer a <i>"light approach"</i></li> </ul>

## Appendix 13: RQ3 - Internal risk reporting and provision of information

Company/Topics	Reporting Line	Frequency and Timing	Content	Use of Visual Tools
<b>Colruyt</b>	<ul style="list-style-type: none"> <li>- RM team → CEO (= chairman of the board) &amp; COO &amp; CFO (ExCo)</li> <li>- RM team → AC → board</li> </ul>	<ul style="list-style-type: none"> <li>- on a quarterly basis</li> <li>- operational units: annual review of risk score and every six months a follow-up</li> </ul>	<ul style="list-style-type: none"> <li>- results of the Coris programme</li> <li>- key risks</li> <li>- for each domain: risks, risk categories, risk scores and their evolution over time</li> </ul>	<ul style="list-style-type: none"> <li>- risk matrices: risk score based on impact and likelihood</li> <li>- risk universe: categorization of the risks</li> <li>- <i>"push the button to see the risks"</i></li> </ul>
<b>Proximus</b>	<ul style="list-style-type: none"> <li>- Director of ARC → CCAO (ExCo)</li> <li>- Director of ARC → AC → board</li> <li>- RM committee → CCAO (ExCo)</li> <li>- RM committee → AC → board</li> </ul>	<ul style="list-style-type: none"> <li>- weekly meetings</li> <li>- a lot of face-to-face interaction between director ARC and ExCo</li> <li>- director ARC attends quarterly AC</li> </ul>	<ul style="list-style-type: none"> <li>- key risks and associated information</li> </ul>	<ul style="list-style-type: none"> <li>- risk scorecards: probability, impact, velocity, BU level, mitigating actions, KRIs, early warnings and risk owner</li> <li>- wants to increase the use of scorecards</li> </ul>
<b>Raffinerie Tirlémontoise</b>	<ul style="list-style-type: none"> <li>- plant managers → safety and environmental coordinator → director of legal department → CEO (→ German director of legal department Südzucker)</li> <li>- CEO + RM department Südzucker → board of R.T.</li> <li>- dir. of legal dep. attends board meetings as secretary</li> </ul>	<ul style="list-style-type: none"> <li>- reporting from the director of the legal department: especially operational risks from the plants</li> <li>- strategic risks are discussed during the executive board meetings</li> </ul>	<ul style="list-style-type: none"> <li>- reporting towards CEO: 2/3 times a month (mainly through personal communication)</li> <li>- reporting towards the board of R.T.: on a quarterly basis</li> </ul>	<ul style="list-style-type: none"> <li>- aware of the existence</li> <li>- do not use them</li> </ul>
<b>Ardo</b>	<ul style="list-style-type: none"> <li>- <i>"We do not really make use of formal reporting systems"</i></li> <li>- every division reports to the ExCo</li> <li>- ExCo reports the key risks to the board</li> </ul>	<ul style="list-style-type: none"> <li>- informal information sharing and transparency between executive level and board level because of the close family ties</li> </ul>	N/A	N/A
<b>Company A</b>	<ul style="list-style-type: none"> <li>- risk manager → CEO &amp; CFO (ExCo)</li> <li>- <i>"the corporate risk manager is an independent function with easy access to the top"</i></li> <li>- AC → board</li> <li>- risk manager: stand-by at board meetings</li> </ul>	<ul style="list-style-type: none"> <li>- informal information exchange</li> <li>- open and accessible culture</li> <li>- very frequent reporting</li> <li>- risk manager: stand-by at board meetings</li> <li>- AC quarterly reports to the board</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- only used in discussions in the executive committees</li> <li>- room for improvement</li> </ul>
<b>Company B</b>	<ul style="list-style-type: none"> <li>- internal auditor → general manager</li> <li>- internal auditor → AC → board</li> <li>- secretary general is informed</li> </ul>	<ul style="list-style-type: none"> <li>- on a quarterly basis</li> </ul>	<ul style="list-style-type: none"> <li>- key risks</li> <li>- not too much information</li> </ul>	<ul style="list-style-type: none"> <li>- colours for maturity levels &amp; risk profiles</li> <li>- overview: processes + risk profile, impact, probability, risk owner etc.</li> </ul>
<b>Company C</b>	<ul style="list-style-type: none"> <li>- risk manager → CFO &amp; CEO (ExCo) → AC → board</li> <li>- risk manager → treasury</li> <li>- risk manager attends part of the AC</li> </ul>	<ul style="list-style-type: none"> <li>- risk manager reports on a quarterly basis to ExCo and AC</li> </ul>	<ul style="list-style-type: none"> <li>- top 10/top 20 risks to CEO and CFO: content remains quite stable over time</li> <li>- weakness: strive for general consensus on the reported risks</li> </ul>	<ul style="list-style-type: none"> <li>- internal risk register</li> <li>- colour codes, risk scorecards</li> <li>- risk is measured on likelihood and impact: both the inherent risk and the managed risk</li> </ul>
<b>Company D</b>	<ul style="list-style-type: none"> <li>- RM department → CFO (ExCo)</li> <li>- RM department → AC → board</li> </ul>	<ul style="list-style-type: none"> <li>- reporting to the AC on a quarterly basis</li> <li>- reporting to CFO happens just occasionally: <i>"The CFO is just part of the standard reporting lines"</i>.</li> </ul>	<ul style="list-style-type: none"> <li>- towards AC: written reports, presentations and financial reports</li> <li>- centrally managed data warehouse and repository with information on internal controls and actions: monthly follow-up</li> </ul>	<ul style="list-style-type: none"> <li>- risk and control matrix for every risk area: too detailed to report</li> <li>- risk map per area: maturity level, evolution over time, date of last audit</li> <li>- risk scorecard per risk: risk owner, initial # of issues, evolution etc.</li> </ul>

## Appendix 14: RQ4 - Determinants

Company/ Det.	Firm Size	Type of Industry	Complexity	Ownership Type	Board Charcs.	Other Determinants
<b>Colruyt</b>	- large company → most advanced ERM programme	- no influence of the industry on the RM system: <i>"the basic steps of the process always remain the same, regardless of the sector"</i> + sharing best practices - impact of the type of risks - roles and responsibilities depend on the type of organisation	- complexity of the group (diversification and globalisation) → increased attention to RM	- family business → <i>"When it is your own money ... you will deal more carefully with risks"</i> + <i>"a certain risk aversion"</i> - no impact of the Corp. Gov. Code: <i>"compliance is not our driving force to install certain things"</i>	N/A	- increased attention to RM at the request of the chairman of the board - <i>"One of the most important key success factors that determine whether your programme stands or falls, is the overall support, assistance, belief and mindset of the top"</i> , <i>"condition sine qua non"</i> - support of the top → no CRO needed - other success factor: <i>"personal involvement on the field"</i> - <i>"the entire approach depends on the support from the top, the company culture ..."</i>
<b>Proximus</b>	N/A	- share best practices with other Belgian companies, benchmarking - telecommunications: attention to data privacy and security - new EU law: GDPR	N/A	- <i>"According to me, there is a large difference between companies listed on the BEL20 and other companies"</i> - Corp. Gov. Code → redevelop systems - Belgian State: no influence	N/A	- growing importance of ERM → redevelop risk systems - board: RM is very important
<b>Raffinerie Tirllemontoise</b>	- not really an influence on RM	- company has to comply with regulations - new legal obligations relating to the environment and security - <i>"IT security has become a hot topic"</i> - food safety is a key risk → department of quality gets bigger - sharing best practices to strengthen the company	- <i>"The more BUs, the larger the exposure to risks"</i> - impact on number of risks, structure of RM remains the same	- large influence of Südzucker: <i>"The strategy, guidelines and procedures for RM are now completely determined by our parent company"</i> → integration → synergies - Südzucker controls the company's RM → no CRO needed	- delegates of Südzucker	- massive explosion in sugar factory → start of RM - support of the top (Südzucker) for RM: <i>"We have a good and correct system which is supported by the management"</i> + <i>"leadership by example is very important"</i> - German Corp. Gov. Code → RM requirements for Südzucker - limited impact of terrorism
<b>Ardo</b>	- substantial size; however no formal RM systems, but own rules & procedures to cover risks	- sector allows the company to cover risks in a natural way: spread activities across different markets - <i>"Food sector is a quite stable industry"</i>	- activities are geographically spread: natural way of covering risks	- <i>"Whether or not your company is publicly traded, every company faces a wide range of risks and uncertainties"</i> - family business: <i>"All shareholders know the company and everything is being discussed in an informal way"</i> + no formal reporting systems	- family members	- impact of the ever-changing world

Company/ Det.	Firm Size	Type of Industry	Complexity	Ownership Type	Board Charcs.	Other Determinants
Company A	N/A	<ul style="list-style-type: none"> <li>- plenty of rules and regulations</li> <li>- data security and privacy are very important</li> <li>- new EU law: GDPR</li> <li>- no fundamental differences with other sectors</li> <li>- sharing best practices</li> </ul>	<ul style="list-style-type: none"> <li>- activities are spread across the world → weakens the different risks</li> </ul>	<ul style="list-style-type: none"> <li>- no significant influence of the stock notation</li> <li>- <i>“anonymous organisation”</i>: different corporate culture compared to family businesses</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- rector of the KU Leuven: trigger for RM</li> <li>- RM is strongly supported by the top → no need for a CRO</li> <li>- influence of the reorientation of activities → increased awareness for RM</li> <li>- influence of the geopolitical situation, the ever-changing world</li> <li>- the crisis → a lot of instability</li> <li>- <i>“If a certain person disappears, the structure will not necessarily remain the same”</i></li> </ul>
Company B	<ul style="list-style-type: none"> <li>- smaller company: less developed RM systems</li> <li>- small company: larger influence of regulations related to the stock exchange listing</li> </ul>	<ul style="list-style-type: none"> <li>- data security and privacy</li> <li>- new EU law: GDPR</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- publicly listed company → compliance with regulations: AC is obliged</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- attention to RM since the merger</li> <li>- loss-making projects underlined the need for more efficient risk assessments</li> <li>- crisis: no significant impact</li> <li>- board: controlling role, no real support for RM</li> <li>- interviewee: support of the top is important to carry people with you</li> </ul>
Company C	N/A	<ul style="list-style-type: none"> <li>- company has to comply with Belgian and European regulations</li> <li>- <i>“Risks are varying depending on the industry”</i></li> <li>- <i>“RM approach depends on the impact on your business processes”</i></li> <li>+ <i>“Your business processes determine on which risks you will focus”</i></li> <li>- data security is important</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- private company, but it also has to comply with multiple regulations: AC is obliged</li> <li>- <i>“Everything is independent of the shareholding”</i></li> <li>- <i>“The Belgian State is not actively managing the company, they do not intervene”</i></li> <li>- <i>“Anglo-Saxon shareholders are very sensitive for certificates”</i></li> </ul>	<ul style="list-style-type: none"> <li>- Belgian State has a right of veto and appoints the chairman of the board</li> </ul>	<ul style="list-style-type: none"> <li>- corporate culture: determines whether people work safely + determines whether risks are being identified</li> <li>- <i>“culture and ownership are the key words”</i>: the company has to be in touch with RM and responsibilities need to be delegated</li> <li>- compliance is often the incentive to do things</li> <li>- impact of terrorism</li> <li>- bond issue → RM is very important for the company's creditworthiness</li> </ul>
Company D	<ul style="list-style-type: none"> <li>- separate RM department</li> </ul>	<ul style="list-style-type: none"> <li>- telecommunications: data security is very important</li> <li>- new EU law: GDPR</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- Corp. Gov. Code → establishment of AC</li> <li>- Large influence of the majority shareholder: has to comply with the SOX (US): risk control framework + increased risk awareness</li> </ul>	N/A	<ul style="list-style-type: none"> <li>- not enough support from the top: RM needs more resources</li> </ul>

## Appendix 15: RQ4 – Summary table

Company/ Determinants	Firm Size	Type of Industry	Level of Regulation	Complexity	Ownership Type	Board Characteristics	Support from the Top	Disruptive Global Events
Colruyt								
Proximus								
Raffinerie Tirlemontoise								
Ardo								
Company A								
Company B								
Company C								
Company D								

LEGEND	
Strong impact	
Moderate impact	
No impact	

## Appendix 16: RQ5 - Consequences of risk oversight

Company/Topics	Impact on the Company's Results	Impact on the Company's Risk Culture
<b>Colruyt</b>	<ul style="list-style-type: none"> <li>- added value for the company: positive impact on the operations</li> <li>- no measurement of the exact impact on the results</li> </ul>	<ul style="list-style-type: none"> <li>- increased internal awareness for RM</li> <li>- no increase in risk aversion</li> </ul>
<b>Proximus</b>	<ul style="list-style-type: none"> <li>- positive influence of controlled risk-taking on the return for shareholders</li> <li>- a lot of synergies from the merger of RM and internal audit</li> </ul>	<ul style="list-style-type: none"> <li>- growing awareness for ERM over the years: <i>"Solely focusing on operational risks does not suffice"</i></li> </ul>
<b>Raffinerie Tirlemontoise</b>	<ul style="list-style-type: none"> <li>- no notion of the added value of RM for the company</li> <li>- <i>"difficult exercise"</i></li> <li>- less internal accidents so they assume it has a positive influence</li> </ul>	<ul style="list-style-type: none"> <li>- awareness campaign</li> <li>- significant impact on risk culture</li> <li>- more risk averse</li> </ul>
<b>Ardo</b>	<ul style="list-style-type: none"> <li>- company uses a natural way of reducing its risks: spreading activities across different countries and different type of vegetables and fruit</li> <li>- no formal RM system/structure → no impact on the results</li> </ul>	N/A
<b>Company A</b>	<ul style="list-style-type: none"> <li>- mature level of RM</li> <li>- a step ahead of new regulations → cost savings</li> </ul>	<ul style="list-style-type: none"> <li>- everyone is aware of the importance of RM</li> <li>- disadvantage of their early lead: very traditional systems</li> </ul>
<b>Company B</b>	<ul style="list-style-type: none"> <li>- difficult to measure</li> </ul>	<ul style="list-style-type: none"> <li>- sometimes the opposite effect: increase in risk aversion</li> <li>- possible solution: development of a risk portfolio</li> </ul>
<b>Company C</b>	<ul style="list-style-type: none"> <li>- RM is important for the firm's credit rating (bond trading)</li> <li>- <i>"Actually, the impact of the attacks was not that big, since a substantial part of it was covered in advance"</i> (of course the human consequences were a lot worse)</li> <li>- report credit rating agency mentions the firm's resilience or flexibility</li> </ul>	<ul style="list-style-type: none"> <li>- substantial increase in the awareness for RM</li> <li>- <i>"Colleagues are more likely to come to me and they appreciate my contribution"</i></li> <li>- more resources are allocated to RM</li> </ul>
<b>Company D</b>	<ul style="list-style-type: none"> <li>- new systems and practices have a positive influence on the operational results: e.g. detection of revenue leakage</li> <li>- benefits primarily occur during the first years of implementation</li> <li>- impact on the results is often invisible because of RM's preventive character</li> </ul>	<ul style="list-style-type: none"> <li>- change in minds of the people: increased awareness for RM</li> <li>- they understand that formal structures &amp; systems are necessary</li> </ul>

