LUND UNIVERSITY
School of Economics and Management

Lund University, School of Economics and Management
Department of Business Administration

BUSN68
Business Administration
*Degree project: Accounting and Management Control*

# Enterprise Risk Management - The usage of COSO's framework in recently publicly listed Swedish companies

Authors:
Josephine Ewerbring
Fredrik Klingvall

Supervisor:
Anna Glenngård

24 May 2016

# ABSTRACT

**Seminar date:** 30 May 2016

**Course:** BUSN68 Business Administration - Degree project: Accounting and Management Control

**Authors:** Josephine Ewerbring and Fredrik Klingvall

**Advisor:** Anna Glenngård

**Keywords:** Risk management, Enterprise Risk Management, COSO, Legitimacy theory, Contingency theory

**Purpose:** The aim of the thesis is to develop previous knowledge of how ERM is used by Swedish listed companies and fill a gap in existing research. More specifically, the thesis explores experiences and possible difficulties from using the COSO framework among newly publicly listed companies.

**Methodology:** A multiple case study of Swedish newly publicly listed companies is conducted, taking an inductive approach and using semi-structured interviews.

**Theoretical perspectives:** The theoretical perspectives are divided in two sections, a practical and a theoretical framework. The practical framework describes COSO's frameworks and the theoretical framework includes stakeholder theory, legitimacy theory and contingency theory.

**Empirical foundation:** In the empirical chapter of the thesis data from the qualitative case study with three case companies is presented.

**Conclusions:** Companies use COSO's framework differently, contingent upon its business context and its circumstances and the difficult phase of ERM will be for companies to ingrain the new risk management practices in the company and making sure that the employees actually complete them.

# PREFACE

This master thesis focusing on Enterprise Risk Management is written by two students at Lund University School of Economics and Management, spring semester 2016.

We would like to thank our supervisor Anna Glenngård for her support and guidance throughout the process of writing this thesis. Furthermore, we would like to thank all of those who have participated in interviews for the result of this thesis. Lastly, we would also like to thank Doctor Rolf Larsson at Lund University and Associate Risk Consultant Jonas Wendt at PwC for their inspiration and assistance in narrowing down the study in this thesis.

*Josephine Ewerbring*
*Lund, May 2016*

*Fredrik Klingvall*
*Lund, May 2016*

# TABLE OF CONTENTS

# GLOSSARY AND ABBREVIATIONS

**Annual Accounts Act** Årsredovisningslagen

**COSO** The Committee of Sponsoring Organizations of the Treadway Commission is a joint initiative dedicated to providing thought leadership to executive management and governance entities on critical aspects on enterprise risk management, internal control and fraud deterrence.

**CFO** Chief Financial Officer

**CRO** Chief Risk Officer

**ERM** Enterprise Risk Management

**IPO** Initial Public Offering

**SEC** Securities and Exchange Commission

**SOX** Sarbanes-Oxley Act

**Confederation of Swedish Enterprise** Svenskt Näringsliv

**PCAOB** Public Company Accounting Oversight Board

**The Swedish Corporate Governance Board** Kollegiet för Svensk Bolagsstyrning

**The Swedish Parliament** Sveriges Riksdag

## APPENDICES



## LIST OF FIGURES AND TABLES

# 1. INTRODUCTION

*In this chapter, a background of risks, risk management and regulation will be presented. Moreover, a problem discussion will be brought up leading to the purpose of the thesis.*

## 1.1 The occurrence of risk

Risk permeates human beings' all endeavours and actually our entire existence. Despite risks' ubiquity, or perhaps because of it, there is no universal definition of risk (Damodaran, 2008). Much like human beings, companies' operations are subject to risks. Countless of companies have defaulted in the recent fraud scandals and financial crises. The dot-com bubble and the accounting scandals in the 21st century related to companies such as Enron, WorldCom, etc. brought down numerous companies. Furthermore, the crisis of 07/08 brought the entire world economy to its knees. In 2015, Romney and Steinbart explain that surveys show that "67% of companies had a security breach, over 45% were targeted by organized crime, and 60% reported financial losses" (2015, p. 123). Risks have been, and always will be ubiquitous for human beings and companies alike.

## 1.2 Risk regulation

In the past centuries, as society has evolved and companies emerged, human beings have learnt how to separate our physical existential risk from economic risk. Moreover, we have lately learnt how to classify risks for businesses (Damodaran, 2008). A common classification of risk for businesses is that of firm-specific risk and market risk. Other risk frameworks divide risks for companies further into hazard, operational, financial and strategic risks (Andersen & Winther Schrøder, 2010). The propensity to classify and manage risk has increased after the crashes mentioned above and as a response governments across the world have introduced legislation and regulation for risk handling within companies. However, the first studies of risk management began after the 2nd World War (Dionne, 2013). Risk management has since then developed over time, going from a Traditional Risk Management (TRM) to Enterprise Risk Management (ERM). TRM mainly focused on investigating silos subject to risk within a company, limiting the risk management since the correlation between the different silos and the enterprise-wide effects on the company were missed (Dornberger, Oberlehner & Zadrazil, 2014). ERM takes a

holistic, portfolio, view of risk management. After the Enron and WorldCom scandals the Sarbanes Oxley Act (SOX) was introduced, primarily to protect public interest by reforming auditing of US publicly listed companies (Pautz & Washington, 2009). SOX makes the executive management and the board of directors more responsible for corporate risk and addresses concerns about corporate reporting by enhancing the oversight of financial accounting (Dornberger et al., 2014). The main implication for companies became the ones stated in Section 404 which focuses on internal control that relates to financial reporting for companies (Securities and Exchange Committee (SEC), 2008). In connection to the enactment of SOX the SEC introduced mandated use of established control frameworks as well as disclosure of internal control weaknesses for publicly listed companies (Romney & Steinbart, 2012). The Public Company Accounting Oversight Board (PCAOB) and the SEC recommends the usage of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) internal control framework (IC framework) for handling the new requirements (The Institute of Internal Auditors, 2008). According to COSO, internal control is "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance (2013, p. 3). COSO is an organisation that provides "thought leadership and guidance on internal control, Enterprise Risk Management (ERM) and fraud deterrence" and it has created two frameworks, which will be further described in the *3. Practical Framework* of this thesis (Protiviti, 2014, p. i). The financial crisis of 07/08 increased people's awareness of the importance of risk management further from the perception people had from the SOX enactment and not only in the US – the previous silo-based approach of TRM became further replaced by ERM (Dornberger et al., 2014). However, according to the Confederation of Swedish Enterprise (2007), COSO's frameworks for internal control and ERM was already gaining acceptance as a global standard as early as in 2007. COSO's frameworks are the most established frameworks in the areas of internal control and ERM (The Institute of Internal Auditors, 2008). For simplification reasons the two COSO frameworks will be referred to as "the COSO framework" but will be separately elaborated in the *3. Practical Framework*.

## 1.3 Swedish regulation and legislation

In Sweden, the Swedish Code for Corporate Governance (the Code) was introduced in 2005, which has similarities to SOX and was introduced rather late compared to similar legislation and codes in the UK and the US (Bylund & Haggren, 2006; Pautz & Washington, 2009). The purpose of the Code is to increase the trust in Swedish publicly listed companies by promoting a positive development of corporate governance. The Code is a complement to legislation and is a standard that is part of the industry's self-regulation. (The Swedish Corporate Governance Board, 2015) Even though the usage of established control frameworks is not mandatory for internal control purposes in Sweden, as it is for publicly listed companies in the US, Swedish companies still use frameworks for corporate governance, risk and internal control handling. Furthermore, much like the US, Swedish companies use the COSO framework (Bonnefond & Lounkokobi, 2007). In addition to the Code, publicly listed companies in Sweden are subject to legislation in the Annual Accounts Act 1995:1554. The section of the corporate governance report in the Annual Accounts Act 1995:1554 states that publicly listed companies should present the most important aspects of the company's internal control and risk management that affects the financial reporting, in the corporate governance report section in their annual report (the Swedish Parliament, 2016). Hence, when listing on a stock exchange for the first time, initial public offering (IPO), not only are companies subject to increased pressure from potential shareholders to increase transparency and disclosure practices but they also become subject to increased legislation and regulation. Fung explains that "corporate governance in today's global environment has become more complex and dynamic in recent years due to increased regulatory requirements and greater scrutiny, creating increased responsibilities for board of directors to comply with rigorous governance standards and also to cope with increasing demand from shareholders and other stakeholders for T&D [Transparency and Disclosure] " (2014, p. 72). Wendt (2016) explains that IPOs are common catalysts for implementing more formal processes for financial reporting within firms, which is due to regulatory requirements.

## 1.4 Problem discussion

According to the Swedish Corporate Governance Board (2015), the trust for companies among legislators and society is crucial for companies to realise their strategies and for them to create

value. COSO's framework's prevalence in the business community is a result of SOX, which purpose was to restore public confidence and enhance the reliability of companies' financial reporting (EY, 2012). Furthermore, the founding principle of ERM is that "every entity exists to provide value for its stakeholders" (COSO, 2004, p. 1). All entities experience uncertainty and management's challenge is to decide the acceptable level of uncertainty when creating stakeholder value. ERM allows management to deal with the inherent uncertainty of conducting business in order to allow the creation of value. (COSO, 2004) Hence, if ERM is implemented in a correct manner an organisation's shareholders can gain vast benefits in terms of shareholder value. Few studies have covered the topic of difficulties when implementing ERM practices though. Dornberger et al. (2014) concluded that there are five main causes of mistakes when implementing ERM, which are: The system itself can be inappropriate, human errors, environment complexity, challenges of identifying risks and finally setting up the metrics. Additionally, consulting firm BaxterBruce (2013) explained that ERM implementation requires commitment of company resources and that it can be time-consuming, among other things. As a result of these difficulties, companies use ERM differently within each organisation even though that companies potentially use the same framework for ERM. COSO have a vague definition of ERM in order for it to suit the risk management of companies in vastly different contexts and this result in differences in usage (COSO, 2004). Indeed, COSO (2003) states that small and large companies implement the COSO framework differently.

However, there are surprisingly few studies on how companies that use COSO's framework use ERM within their organisation and what the main difficulties have been for them. Hence, this will be the locus of the thesis.

## 1.5 Previous studies

Previous studies have focused on investigating the usage of COSO's IC framework between different companies and the ones which have focused on usage of ERM by different companies, have been rather limited in depth. The previous studies of ERM have primarily interviewed the Chief Risk Officer (CRO) (or the person with the final responsibility of risk management) within the investigated companies and considering that ERM should permeate an entire organisation,

additional studies covering different hierarchical levels are needed in this area. For example, a study by Berg and Skoog (2012) of Andra AP-fonden and Astra Tech had this limitation and they suggested further in-depth research into the different levels of companies. Another study by Isaksson Fagerudd et al (2011) did go in-depth of the internal control practices of SEB, a bank, but it did not focus on ERM but instead on COSO's IC framework. Furthermore, the studies specifically focusing on the difficulties of using ERM are surprisingly few.

## 1.6 Purpose and research focus

The aim of the thesis is to develop previous knowledge of how ERM is used by Swedish listed companies and fill a gap in existing research. More specifically, the thesis explores experiences and possible difficulties from using the COSO framework among newly publicly listed companies.

## 1.7 Structure of the thesis

In order to fulfil the purpose of the thesis, an adequate study needs to be undertaken and background information for the study will be provided in Chapter 1. In Chapter 2, the method used to approach the study and collect empirical material is presented. Once the method has been explained the practical framework explaining COSO's two frameworks is brought up in Chapter 3. The chapter of the practical framework is followed by Chapter 4, which explores relevant theories for analysing the result of the thesis, that is the Stakeholder theory, Legitimacy theory and Contingency theory. Chapter 5 presents the empirical material of the thesis, which is based on a multiple case study of three companies. An analysis of the empirical material is conducted in Chapter 6, by using the practical and theoretical framework from Chapter 3 and Chapter 4. Lastly, a broad discussion of ERM and COSO's framework is held in Chapter 7, which also ends with a conclusion.

# 2. METHODOLOGY

*This study is based on a multiple case study. In this chapter the rationale for the chosen cases and the data used to fulfil the purpose of the study is presented. Furthermore, argumentation of why the method is suitable for our study will be conducted.*

## 2.1 Qualitative case study

In order to fulfil the purpose of this thesis, the best approach to investigate the ERM usage of companies would be to take an inductive approach. The reason for taking an inductive approach is because the theory in the research area is considered incomplete and it would be inappropriate to state hypotheses, which are tested, considering the few studies covering this specific topic. However, the study will have tendencies of deductivism, since previous theory exists and we have developed a relatively clear theoretical position before the collection of data in the study. Bryman and Bell (2011) explain that it is important not to overstate how static the approach is, inductive or deductive, considering the approaches are mere tendencies and not definitive correspondence. The research strategy chosen to fulfil the purpose of the thesis is a multiple case study using qualitative data.

According to Bryman and Bell (2011) it is helpful to distinguish between qualitative and quantitative studies, even though the distinction might sometimes be ambiguous. This study of ERM took a qualitative research strategic approach. The study used interviews where the interpretation of conversations was the bedrocks of the analysis. According to Saunders, Lewis and Thornhill (2009), qualitative data is non-numerical data that is expressed through words that is used to find answers to the stated research question, by analysing the findings and collecting evidence not known in advance, which is applicable to this study. A qualitative research strategy was used due to the fact that a deep understanding of the situation of the case companies being studied was aimed at. In order to gain the deep understanding that was aimed at, case studies was selected as a method.

As has been concluded, there are surprisingly few studies focusing on the difficulties when using ERM within companies. The case study method was therefore chosen in order to drill deep into

the practical usage of ERM of specific case companies. The aim was to gain rich descriptions of how ERM is being used and what difficulties affect the usage of ERM for publicly listed companies. According to Yin (2012), the case study method is pertinent when a descriptive research question is used and surveys should not be used when rich information is needed in the study. Hence, the case study method is considered appropriate in the case of this thesis.

## 2.2 Literature review

The literature used in this thesis was found through research on search engines LUB Search, Google Scholar, Lund University library search system as well as through the general search engine Google. Relevant scientific articles were found through these search engines. In order to delimit the range of literature and to capture the relevance of it, the researchers looked for keywords such as "Enterprise Risk Management", "COSO", "COSO ERM" "COSO ERM implementation", "controlling" etc. When conducting the literature review, we began by investigating the theories of risk management, following up on the development of these theories to observe changes within them. Appropriate concepts and theories were central in the selection for the further development of a study. The theories were selected in order to be able to analyse the empirical material and thereby understand the findings from a theoretical point of view and thereby also fulfil the purpose of the thesis.

## 2.3 The Case study

The data was collected through a multiple case study through semi-structured interviews with employees within three case companies. The reason why semi-structured interviews were used, instead of structured interviews, was due to the increased freedom when asking questions to the respondents, to thereby gain a deeper understanding of the ERM practices within the specific case companies (Bryman & Bell, 2011). Hence, semi-structured interviews allowed for depth of the study. An explanation of the selection of the respondents within each case company can be found in the *2.4.2 Sampling* section in this thesis.

### 2.3.1 Case selection

To fulfil the purpose of the study, three case companies were selected for the study. The criteria the case companies had to fulfil were several, as we wanted the three's characteristics to be as comparable as possible to each other to enable an analysis of their ERM connected to the companies' characteristics. In order to select specific companies multiple steps were taken.

**Step 1**

Firstly, we contacted Jonas Wendt, Risk Associate at Pricewaterhousecoopers (PwC), which was possible since we had previous contact with Mr Wendt in other business related contexts. To view the interview questions posed to Mr Went, please view *Appendix 1*. The reason we contacted a professional at PwC was because PwC has collaborated extensively with COSO in the construction of their framework. For example PwC lead the project and was the authors for the updated 2013 IC framework (COSO, 2013). Moreover, a predecessor of PwC collaborated with COSO in the construction of the 1992 IC framework (COSO, 2013). The aim of the interview was to present our thesis idea and to get background information of how different companies use COSO's framework. This, in order to be able to decide which companies to choose for the study. A discussion of the COSO framework and the feasibility of our study were held. Wendt explained that companies usually start focusing more on risk management ones they become publicly listed companies; "a catalyst for many for starting to view risk management from a broader perspective is an initial public offering" (2016). Wendt further explained that that is due to the increased regulation for publicly listed companies, for example the requirements in Annual Accounts Act 1995:1554 (Wendt, 2016). Additionally, Wendt (2016) explained that not all companies have a Chief Risk Officer (CRO) and recommended us to speak to the CFOs when first contacting our potential case companies. This was taken into consideration when later contacting the case companies and sampling the respondents for the study. After the interview with Wendt (2016), we decided to narrow down the list of potential companies to companies that had completed an IPO on the Nasdaq OMX Stockholm Stock Exchange between 2014-2016 (Nasdaq, 2016). The Nasdaq OMX Stockholm Stock exchange was chosen to limit the study to Swedish companies and the time between the years 2014-2016 was considered suitable since it allowed the researchers to investigate ERM usage of newly publicly listed companies.

**Step 2**

Secondly, to narrow down the number of case companies, the financial services sector IPOs were excluded, considering that financial services companies in Sweden have increased regulation on risk management from the Financial Supervisory Authority (FI, n.d.). Thirdly, the case companies had to be publicly listed fairly close to each other in order for their implementation of increased risk management to be in a similar state (time wise). Fourthly, the companies had to be of roughly similar size (in terms of sales and number of employees). Fifthly, and lastly, in order to ensure that the case companies used the COSO framework, the annual reports leading up to the IPO, as well as the annual reports after the IPO, of the potential case companies were investigated. Multiple companies used a version of the COSO framework according to their annual reports and were therefore selected as potential case companies that should be contacted in the study. Three companies hereafter referred to as Company 1, Company 2 and Company 3 (due to anonymity requests) responded positively (in terms of wanting to participate) to us when we reached out to them.

**Step 3**

Considering that the annual reports only indicated whether the companies used COSO's framework and ERM practices, a further investigation had to be made to ensure the suitability of the three potential case companies (Company 1, Company 2 and Company 3).

First, the case companies' risk responsible or CFO was contacted over phone for a brief telephone interview and description of the study and thesis. We chose to speak with the CFO for Company 1 since there was no indication that the companies had a Chief Risk Officer or similar, which is also in accordance with what Wendt (2016) mentioned. The Chief Audit Executive of Company 2 was contacted in the case of Company 2. The CFO was contacted in the case of Company 3 for the same reason as for Company 1. Semi-structured interviews were held over phone for approximately 5 minutes with the CFO or Chief Audit Executive, with no recording. The reason for not recording the conversation was because of the perceived sensitivity of the conversation from the interviewee's point of view. They could not verify whom they were talking to and had no information of what the study being conducted was about. All three companies were deemed suitable for the study after the brief telephone interviews.

**Step 4**

Considering that all three companies seemed to be using the COSO framework as well as having a strategic thinking regarding risk, the three companies were selected for the study. Moreover, as the aim of the study was to investigate the usage of ERM (which should permeate the organisation), the researchers asked for interviews with several people within the company. Firstly, the person who is in charge of ERM (CRO or CFO), secondly, an employee that is affected by it (Financial Assistant or similar). Hence, we chose to interview two employees within each case company. The exception to this was Company 2, which did not have the resources at the time of the interviews to provide us with additional sources than that of the Chief Audit Executive.

## 2.4 Conducting the case study

### 2.4.1 Case company description

Due to the sensitivity of the data in this thesis, the investigated companies will be referred to as Company 1, Company 2 and Company 3. Furthermore, no detailed description of the companies will be provided in order to maintain the anonymity of the companies. The investigated companies were publicly listed between 2014 and 2016 and are active in different industries. To view an illustration of the time of the IPOs for the specific companies, please view *Figure 1* below. For brief company descriptions, please view *Table 1 below.*

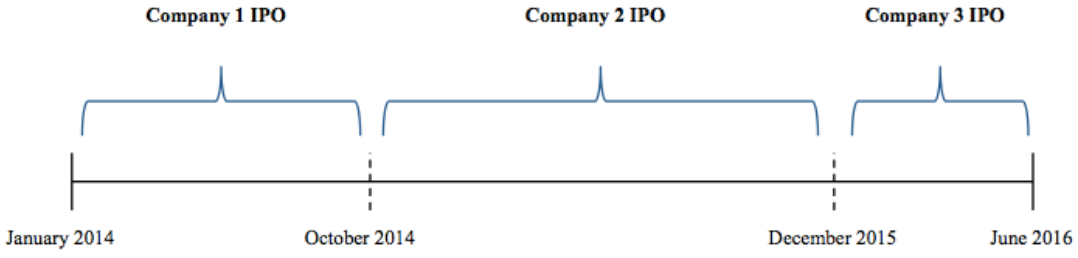


*Figure 1*: IPO Schedule for the case companies

| Company Descriptions | | | |
|---|---|---|---|
| **Company** | Company 1 | Company 2 | Company 3 |
| **Description** | Consolidated to a group close to its IPO and was listed on Stockholm OMX in 2014 | Listed between late 2014 and late 2015 on Stockholm OMX | Listed between late 2015 and mid 2016 on Stockholm OMX. Considered completing its IPO as early as in 2014 |
| **Industry** | Active in the consumer goods industry | Active in the consumer goods industry | Active in the healthcare industry |

*Table 1*: Case company descriptions

### 2.4.2 Sampling

Prior to the conducted study, we investigated the research area in order to develop a relatively clear theoretical position. Based on the previous research in the area, purposive sampling was used to select the appropriate respondents within each case company. In order to be able to evaluate ERM within the organisation as a whole, considering that one of the pillars of ERM is that risk management should be "applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk" (COSO, 2004, p. 2), the criteria for choosing the respondents was contingent upon the specific case company. Furthermore, a theoretical sampling method was used in order to be able to theorise our findings. Theoretical sampling is advocated by Glaser and Strauss, in order to "discover categories and their properties and to suggest the interrelationships into a theory" (Glaser & Strauss, 1967, recited in Bryman & Bell, 2011, p. 431). The following criteria was to be upheld for the respondent to be selected as an interview candidate:

- Top-level: Employee that is responsible for the risk management strategy and practices (CRO or CFO)
- Unit-level: Employee that is positioned in a finance unit and affected by the approach (Financial Assistant or similar)

### 2.4.3 Interview guide

Interview guides, in accordance with Bryman and Bell's (2011) advocacy, were created in order to support the semi-structured face-to-face interviews with the three case companies. An

interview guide was to prefer in our case over a structured interview schedule, which is normally associated with structured interviews, considering that flexibility was beneficial in order to gain a deep understanding of ERM practices of the case companies. Furthermore, the interview questions were posed in Swedish during the interviews since all respondents were native Swedish speakers. Hence, it was done to not miss out on any details or nuances in the answers due to poor communication. To view the interview questions for each of the interviews conducted (available in Swedish and English), please view *Appendix 2-5*. (Bryman & Bell, 2011). However a summarised version can be viewed in *Table 2* below.

| Interview Questions | |
|---|---|
| **Interview Guide sections** | **Example questions** |
| Risk management on a general level | In general how would you describe the risk management practices of the company on a holistic level? |
| Internal Control practices | What is your view on companies internal control environment? Do you work with risk assessment? Etc. |
| Enterprise Risk Management practices | Do you work with risk on a strategic level? How do you view risk in terms of company's risk appetite? |
| Implementation and usage of the framework | Is anything difficult or problematic regarding risks and controls within the company? |

*Table 2*: Interview sections from the Interview Guide

Firstly, an open general question was asked in order to allow the respondent to provide a wide view of the risk management of the company. The idea of the question was to enable follow-up questions on the risk management of the firm, specifically related to the other sections of the interview guide. Secondly, questions were created and divided into the internal control components of the COSO IC framework (which is contained in the ERM framework) to get a picture of where the company was in their usage of COSO's framework and identify where difficulties have emerged in the usage of the framework. The interview questions were further tied to the 17 principles of COSO's IC framework. Thirdly, questions regarding ERM were asked to investigate how they view, and work, with risks and controls on a strategic level. Finally, the interview ended with questions regarding how successful they consider themselves

to be using the COSO framework and if they have experienced any difficulties or problems so far since starting to use COSO's framework.

### 2.4.4 Conducting the interviews

Both authors participated in all interviews in which one acted as the lead interviewer and the other as support interviewer who had the task of making sure that all information that needed to be obtained was collected. The support interviewer did so by having a detailed interview guide, making sure that all topics had been covered. For descriptive statistics, please view *Table 3 below.*

| Descriptive Statistics | | | | | |
|---|---|---|---|---|---|
| **Company** | Company 1 | | Company 2 | Company 3 | |
| **Place of interview** | Headquarters | | Headquarters | Headquarters | |
| **Title of interview subject** | CFO | Financial Assistant | Chief Audit Executive | CFO | Group Financial Controller |
| **Date** | 11 March | 11 March | 21 March | 20 March | 20 March |
| **Time of interview (approx.)** | 55 minutes | 35 minutes | 70 min | 50 minutes | 35 minutes |
| **Interview subject's time at the company, since:** | Beginning of 2014 | Beginning of 2014 | End of 2015 | Beginning of 2012 | End of 2015 |
| **Language** | Swedish | Swedish | Swedish | Swedish | Swedish |
| **Recorded** | Yes | Yes | No | No | No |
| **Notes taken** | No | No | Yes | Yes | Yes |

*Table 3*: Case company descriptive statistics

## 2.5 Data collection

In order to arrive at reliable conclusions based on the purpose, both primary and secondary data were used. Primary data was collected through interviews and secondary data were the companies' annual reports and their IPO Prospectus. Secondary data was used to complement the findings from the interviews.

### 2.5.1. Primary data collection

Primary data increases the level of detail according to Saunders et al. (2009), which allows researchers to target information directly to the real-related research according to Yin (2009). Reliable data was collected through interviews that were relevant to the research topic of this thesis, complying with the purpose. In this thesis, two interview techniques were used, namely, semi-structured telephone interviews and semi-structured face-to-face interviews (Bryman & Bell, 2011: Potter, 1997).

### 2.5.2. Secondary data collection

Secondary data, in the form of the annual reports and the IPO Prospectus of the companies were used to contrast our primary data from the interviews with the case companies. This approach, using multiple sources of information, is recommended by Yin (2009). All annual reports of the case companies that had been published prior to the IPOs, as well as all annual reports that had been published after the IPO, were investigated to identify when a company made its first references to the COSO framework or its components. The specific sections on risk management and control in the corporate governance section of the annual reports were investigated. Moreover, the secondary data was used to identify any potential differences between what the companies communicate in the annual report and the IPO Prospectus and the findings from the case company interviews.

### 2.5.3 Processing the data

In order to draw any conclusions from the study, the data collected was also analysed. The empirical analysis was done by comparing and analysing the empirical findings, both primary and secondary data, with the practical and theoretical framework. Since the interviews were either recorded or since notes were taken, the researchers could go back and forth between the interview material and the result, creating and iterative process in the analysis. Both of the two researchers analysed the material so that the conclusions made could be considered valid.

In accordance with recommendations from Bryman and Bell (2011), we asked if we could record all interviews, however, only Company 1 allowed recording of the interviews. Taking notes were allowed throughout all interviews though. Considering that the researchers not only were

interested in what the respondents said, but also how they said it, audio recording was considered the most appropriate approach. However, as researchers we had to be pragmatic in the case of Company 2 and Company 3 since they preferred us not to record. During these interviews it helped to be two interviewers, one asking questions and one taking notes. Furthermore, in order to ensure that the collected interview data was reliable, respondent validation was completed. Due to the fact that the interviews were not recorded, quotations will not be made in the result of this thesis. Simply, providing quotations of only Company 1 in the result would have tilted the result and put specific weight on Company 1's empirical material.

## 2.6 Validity and Reliability

The study took an inductive approach to fulfil the purpose of the study and when constructing the interview guide meticulous attention was paid in order to maximise the internal validity of the study. According to Bryman and Bell (2011), this ensures high level of congruence between observations and concepts that strengthen the research in the interviews. Moreover, the fact that employees in different hierarchical levels were interviewed increased the validity of the study. As earlier stated, previous studies in the area of ERM was limited to interviewing the CFO or CRO. The external validity is limited though considering that only three companies in one institutional environment, Sweden, have been studied (Bryman & Bell, 2011). If a different international office of the companies were interviewed, perhaps the result would have been different. Hence, in order to allow for generalisability of our study it would have been beneficial to include more case companies as well as having interviewed additional employees in each organisation. However, due to the sensitivity of the data required from the companies in this study (from the companies' perspective) and the limitation on the companies' to open up their human capital in the financial divisions during financial reporting times the study should be considered rigorous, though not generalisable.

The internal reliability of the study is high considering that two researchers conducted the interviews and interpreted as well as analysed the result from them, in order to agree about what has been heard and seen (Bryman & Bell, 2011). Moreover, the result was also sent to the respondents for validation of the correspondence between findings and the empirical material

(Bryman & Bell, 2011). However, the replicability is low considering that semi-structured interviews were conducted where the questions were adapted and contingent on the answers provided by the respondents. Moreover, due to the sensitivity of the information provided by the companies, only one company allowed recordings to be made. Notes were taken during the interviews that were not recorded though.

## 2.7 Limitations

In this case study, several limitations have been encountered. As we chose to answer the purpose based on the practices of only three companies, the result of the thesis is limited. It would have been desirable if the empirical material were collected from a larger sample. However, the research area of this thesis is rather narrow, in terms of companies that recently completed an IPO and have started to use COSO's framework. Hence, the potential sample size was small from the beginning. It is a highly relevant area of research though, considering the increasing prevalence of the COSO framework as well as that companies that lists on a stock market are subject to more regulation and scrutiny in terms of risk.

# 3. PRACTICAL FRAMEWORK - COSO'S FRAMEWORKS

*In this chapter, COSO's two frameworks will be presented. The chapter will also provide the reader with a solid foundation of knowledge to understand ERM of the case companies as well as an indication of how to optimise the usage when starting to use the frameworks.*

As previously mentioned, COSO's frameworks are the most established frameworks in the areas of internal control and ERM and are used by most publicly listed companies in the US (The Institute of Internal Auditors, 2008). COSO is an organisation that provides "thought leadership and guidance on internal control, Enterprise Risk Management (ERM) and fraud deterrence" (Protiviti, 2014, p. i). The first framework by COSO was introduced in 1992 and called Internal Control – Integrated Framework. The framework from 1992 became the predominant IC framework for companies as a result of the enactment of SOX and Section 404 (Protiviti, 2014). Since then the COSO IC framework has been updated ones, in 2013, and an expanded version called Enterprise Risk Management – Integrated Framework (ERM framework) was introduced in 2004 (COSO, 2004). For an illustration of the 2013 IC framework, please view *Figure 2*

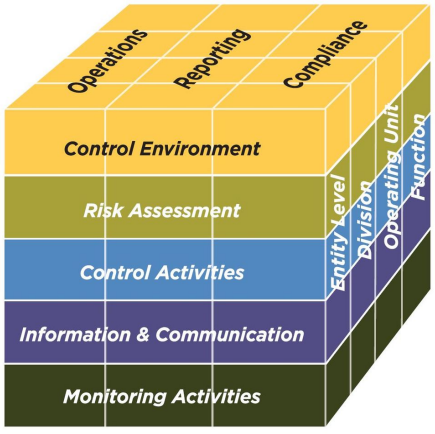


*Figure 2:* COSO's 2013 IC Framework (COSO, 2013)

The IC framework has five components; Control Environment, Risk Assessment, Control Activities, Information & Communication and Monitoring Activities. The five components include 17 principles. To view the 17 principles, please view *Appendix 6.*

The ERM framework was created by COSO because there was no common integrated literature on risk and risk management and there was a need to step out of silo thinking of risk in organisations and instead look at the entire enterprise's risk. Furthermore, the risk thinking did not start with the organisation's' objectives, and then evaluating the risks when trying to achieve the objectives. (COSO at 30 Years, 2015) The relationship between the COSO IC framework and the ERM framework is that the ERM framework is broader than the IC framework. Furthermore, it also encompasses the IC framework within it and should be used by companies wanting to look beyond internal control and increase the return of their effects to the next level (COSO, 2010).

According to COSO the definition of ERM is (2004, p. 2):

- "A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories"

The definition is purposefully broad but the primary focus of ERM is on the achievement of objectives (COSO, 2004). For an illustration of the COSO ERM framework, please view *Figure 3.*

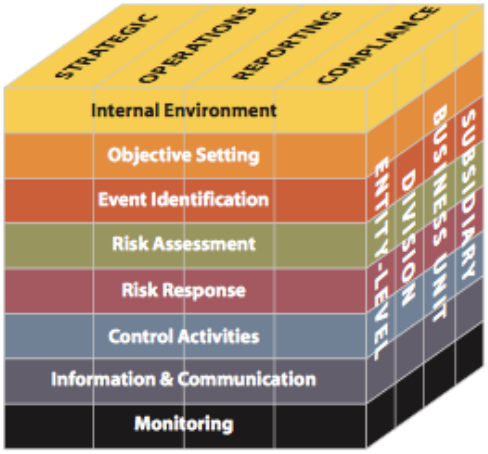


*Figure 3*: COSO's ERM Framework (COSO, 2004)

The ERM framework is broader than the IC framework. The five components are expanded to eight and have slight name changes; Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information & Communication and Monitoring. The components are of similar nature though considering that the IC framework is included in the ERM framework. However, the ERM framework recognise that risk does not have to be completely mitigated but can be "accepted, avoided, diversified, shared or transferred", according to Romney and Steinbart (2015, p. 196). The eight components of the ERM framework will be explained below.

## 3.1 COSO's frameworks' components

### 3.1.1 The Internal Environment

The Internal Environment can be viewed as the company's culture and how this culture influence the strategy, structure and risk management within the organisation. The culture also affects the risk appetite of a firm, risk appetite being "the amount of risk they are willing to accept to achieve their goals" (Romney & Steinbart, 2015, p. 197). In order to be able to avoid improper risk, the risk appetite should be aligned with a company's strategy (Romney & Steinbart, 2015). Therefore it is important to involve the board of directors considering that they not only should consider overall risks in regards to the strategy of the firm, but also because they should have

oversight over the internal control practices according to the Code (The Swedish Corporate Governance Board, 2015).

Moreover, an important aspect in order for a company to achieve its objectives is that the company should assign responsibility and authority to employees within the organisation. This is done by for example using formal job descriptions, employee training, code of conducts etc. Furthermore, Human Resources Management is a crucial aspect for an organisation for it to be able to hire and retain key employees in the organisation. (Romney & Steinbart, 2015)

### 3.1.2 Objective Setting

Management should decide what the company wants to achieve, on a strategic as well as on a corporate and sub-division level within the Objective Setting component in the ERM framework. The importance of objective setting can also be found throughout the COSO IC framework. The most important objective according to COSO is that of creating shareholder value. (Romney & Steinbart, 2015)

### 3.1.3 Event Identification

An event is "an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives. Events may have positive or negative impacts or both." according to COSO (recited in Romney & Steinbart, 2015, p. 201). Hence, an event is characterised by uncertainty and it is therefore hard to determine its impact and likelihood of occurrence. Moreover, events might correlate with each other and should therefore not be considered individually but collectively. Management has to identify all risks and determine their relevance for the organisation. (Romney & Steinbart, 2015)

### 3.1.4 Risk Assessment and Risk Response

The relevance of the risks identified can be evaluated using several models and frameworks but the likelihood and impact is a common model. Furthermore, management should identify controls that can be used to mitigate or prevent risks from occurring. A good internal control system should incorporate preventive, detective and corrective controls in order to be effective. (Romney & Steinbart, 2015)

### 3.1.5 Control Activities

According to Romney and Steinbart (2015), control activities are "policies, procedures, and rules that provide reasonable assurance that control objectives are met and risk responses are carried out" (2015, p. 204). Control procedures can be categorised into the following categories according to Romney and Steinbart (2015):

1. Proper authorisation of transactions and activities
2. Segregation of duties
3. Project development and acquisition controls
4. Change management controls
5. Design and use of documents and records
6. Safeguarding assets, records and data
7. Independent checks on performance

### 3.1.6 Information and Communication

In order to be able to carry out daily tasks, know who is responsible for what, and to be able to achieve the long-term objectives of the company within the risk appetite, communication must be used. Moreover, the risk management and communication practices should not be limited to the organisation, but should also reach external parties such as suppliers. (Romney & Steinbart, 2015)

### 3.1.7 Monitoring

In order to create an effective internal control system it is important to monitor the practices and also modify them if needed. The deficiencies in the system should be reported to management and thereafter to the board of directors. In order to detect deficiencies, audits are an effective activity. Further activities and systems are the use of forensic experts, fraud hotlines, recruitment of compliance officers etc. (Romney & Steinbart, 2015)

## 3.2 Implementation and usage of the frameworks

COSO has issued multiple thought papers on the implementation and usage of the ERM framework and IC framework. The thought paper "Embracing Enterprise Risk Management: Practical Approaches for Getting Started" by COSO explains how to start using ERM (2011). The paper explains that there are several keys to success (COSO, 2011):

1. Provide support from the top
2. Use incremental steps
3. Focus on a small number of risks
4. Leverage existing resources
5. Build on existing risk management activities
6. Embed ERM into the business fabric of the organisation
7. Provide ERM education to senior management

In order to manage risk successfully ERM practices should be taken on, on an enterprise level with a strategic focus. Hence, it is important to involve and gain support from the top management of the organisation since capital has to be allocated to support ERM activities. Furthermore, top management also set the risk culture within the organisation, which have been stressed by credit rating agencies such as Standard & Poor's, as an important part of ERM. (COSO, 2011)

It is common not to implement ERM in one large effort but take it in incremental steps in order to reduce costs and timeliness of the implementation. There are several advantages to this approach such as the achievement of immediate tangible results, tailor made ERM processes and facilitation of evaluation of benefits of each step. Companies usually focus on a small number of risks to later on be able to add an added amount of risks to consider. Furthermore, many organisations are not required to recruit new employees to carry out the ERM practices but have talented staff with the abilities to take on ERM projects. Oftentimes CFOs set up a management committee with existing employees to facilitate the implementation. (COSO, 2011)

Most organisations have existing risk management activities in place and enhancing and expanding these activities can achieve immediate and tangible benefits. However, a portfolio-view of the risks with their correlation in focus should be taken into consideration. Furthermore, as has already been explained, ERM should permeate the entire organisation. Hence, ERM cannot be implemented as a stand-alone function. With that said, assigning responsibility and authority is important. Since ERM is an on-going effort management should get updates on the practices and difficulties within the organisation in terms of ERM. Furthermore, as the organisation develops they will also require training and education in the area of ERM. (COSO, 2011)

## 3.3 Combining the two COSO frameworks in the thesis

For simplification reasons the two COSO frameworks will be referred to as the COSO framework.

# 4. THEORETICAL FRAMEWORK

*In this chapter, theories connected to the purpose of this thesis will be presented. The theories will be divided into 3 main chapters; Stakeholder theory, legitimacy theory and contingency theory, in order to create a complete theoretical framework, which will be used to analyse the results of this thesis.*

## 4.1 Stakeholder theory

Stakeholder theory explains the relationship between an organisation and its internal and external environment and how this relationship influences the way the businesses conduct their activities (Freeman, 1984). Stakeholder theory attempts to widen management's view of its role in society and its responsibilities beyond profit maximisation according to Mitchell et al. (1997), which is contrasting to shareholder theory (Friedman, 1970). The stakeholder theory highlights a fundamental question to the organisation in question according to Mitchell et al., namely "which groups are stakeholders deserving or requiring management attention and which are not?" (1997, p. 855). According to Hill and Jones the term stakeholder refers to "groups of constituents who have a legitimate claim on the firm" (1992, p. 133). Another common definition of a stakeholder comes from Freeman's early definition; "a stakeholder in an organization is (by definition) any group or individual who can affect or is affected by the achievement of the organization's objectives" (Freeman 1984, recited in Mitchell et al., 1997, p. 856). Typical stakeholders include creditors, customers, managers, stockholders, suppliers, general public and local communities according Hill and Jones (1992). For example customers can be considered a stakeholder since they provide the firm with revenue and expect value for their money in return. Moreover, communities can be considered a stakeholder since they provide the firm with locations as well as infrastructure required (Hill & Jones, 1992).

Stakeholders can differ in terms of their importance to a firm in regards to their claim of the firm. Hill and Jones explains that "compared to actors with a low stake in the firm, actors with a high stake will demand more comprehensive incentive mechanisms and governance structures in order to safeguard their asset-specific investments in the firm" (1992, p. 133-134). This notion is supported by Mitchell et al. (1997) which classify the salience of different stakeholders and their

claim on the firm according to three attributes; Power, Legitimacy and Urgency. Furthermore, Mitchell et al. (1997) explain that the stakeholder attributes are variable, socially constructed (not objective) and a stakeholder may not be aware of its stakeholder salience. An additional crucial aspect of stakeholder theory is the role of management. Mitchell et al. (1997) explain that the managers of an organisation determine a stakeholder's salience. Hence, whether a stakeholder gets the attention of management will determine whether the stakeholder becomes salient.

Organisations that manage their stakeholder relationship effectively are more likely to perform and survive longer than organisations that do not understand and nurture their relationships (Freeman, 1984). Certain stakeholder competencies should be developed according to Freeman (1984), these include developing strategies to effectively deal with stakeholders and their concerns, making a commitment to monitor stakeholder interests, ensuring that organisational functions address the needs of stakeholders and dividing and categorising interest into manageable segments. View *Figure 4* for Freeman's view of the stakeholder of a firm.


*Figure 4*: Stakeholders for a firm according to Freeman. (Stormbal, 2016)

However, despite many scholars covering stakeholder theory, little attention has been paid to what creating value means for stakeholders and how they can measure it. Much of the literature assumes that value in this sense is the economic value. However, a significant portion of the value stakeholders perceive from collaborating with stakeholder-friendly firms may not be composed in economic measures per se, some stakeholder might value other measures of value. A stakeholder-based performance measure therefore challenges managers to distance themselves from limiting themselves to creating solely economic value. To instead examine the value creation by their firm in a broader sense and consider all stakeholders and also their contribution to the value creation. (Harrison & Wicks, 2013)

## 4.2 Legitimacy theory

Legitimacy theory has many similarities to stakeholder theory according to Deegan and Unerman (2011) and both theories infers that an organisation is part of a social system in which the organisation impacts, and is impacted by, other groups in society. Hence, the two theories can be considered to be overlapping even though the legitimacy theory focuses on society as a whole, while stakeholder theory focus on the interaction with particular stakeholders (Deegan & Unerman, 2011). According to Suchman, legitimacy is a "generalised perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions" (1995, recited in Deegan and Unerman, 2011, p. 324). Organisations are continuously trying to ensure that they are perceived as "operating within the bounds and norms of their respective societies", according to Deegan and Unerman (2011, p. 323). Furthermore, in line with Mitchell et al.'s (1997) view on the attributes (legitimacy being one of the attributes) as being constantly changing, Deegan and Unerman (2011) explain that the bounds and norms within societies are not considered to be fixed, but changing over time. Legitimacy theory is based on the principle that there is a social contract between the firm in question and the society in which it operates. Previously, traditional profit maximisation was perceived to be an adequate measure of corporate performance, but in recent years significant changes in public opinions have emerged. Heightened social expectations are emerging and in order for society to perceive a company as successful it has to be attentive to human, environmental and other social consequences of its activities. (Deegan & Unerman,

2011) Society as a stakeholder is increasingly expecting businesses to expand its value creation. Failure to comply with the expectations may result in imposed sanctions in the form of legal restrictions on the operations or resources of the company in question, or an impaired demand of the products or services of a company by its consumers (Deegan & Unerman, 2011).

Legitimacy is considered to be a resource on which an organisation is dependent on for its survival, and is also desired by companies to possess (Deegan & Unerman, 2011). Compared to other resources that a company uses, legitimacy is a resource that can be manipulated through disclosure strategies. Strategies aiming at gaining, maintaining or repairing legitimacy are often referred to as legitimation strategies and can include targeted disclosures as well as collaborations with other parties that are perceived by society as legitimate. By collaborating with legitimate organisations a firm can be provided legitimacy by association. (Deegan & Unerman, 2011) According to Suchman (1995, recited in Deegan & Unerman, 2011) there are two categories of strategies for maintaining legitimacy for firms; forecasting future changes and safeguarding previous accomplishments. Lindblom (1993, recited in Deegan & Unerman, 2011) proposes that organisations can use four courses of action as legitimation strategies to obtain, maintain or repair legitimacy, which are: Educate and inform the stakeholders of actual changes of the firm's activities and performance which are in line with society's expectations; Change the perception of the firm's performance and activities but not the actual behaviour of the firm; Deflect attention from the actual issue onto another issue for which the firm has fulfilled the expectations and change external expectations of its performance by convincing the stakeholders that they are unreasonable.

According to Lindblom (1993, recited in Deegan & Unerman, 2011) companies can use their annual reports to execute each of the above strategies. As previously mentioned, increased value on social contributions by companies is valued by society. As a consequence of this, corporate legitimation strategies have increased focus on practices for managing risks in regards to their reputation. Reputation risk management emphasise the financial importance of legitimacy for a firm where reputation is considered a resource for future profits - damages to the reputation affects the future profitability (Deegan & Unerman, 2011).

## 4.3 Contingency Theory

Contingency theory have its foundation in contingency theory of organisational structure which was developed from the 1950s and the theory codified which organisational structures that were most appropriate for specific circumstances (Otley, 2016). According to Donaldson (2001), the core of the contingency theory paradigm is that organisational effectiveness results from the suitability of its characteristics (for example its structure) with contingencies that reflect the situation that the organisation is in and affected by. Contingencies in this sense include the environment, organisational size and organisational strategy. (Donaldson, 2001) Considering that higher suitability of the organisation's characteristics with its contingencies leads to higher performance, organisations will seek to be suitable to its contingencies (Donaldson, 2001). From the 1970's contingency theory of management accounting started to shape and had its foundation in the contingency theory of organisational structure, which had been developed previously. Contingency theory of management accounting attempted to explain the plethora of management accounting practice that was apparent at that time (Otley, 2016).

More recently additional applications of contingency theory have emerged such as its application to explain ERM of companies. Companies across the globe face market risk, operational risk and reputational risk etc. Further increasing the complexity of organisations are mergers, deregulation, global competition and general market shifts. (Nedaei, Rasid, Sofian, Basiruddin & Kalkhouran, 2015) Hence, a business leader has to manage risks in accordance with its company's characteristics, being size and nature of the operations, in order to realise the company's objectives. Despite the fact that risks can take various forms, each risk should not be managed separately and a silo-based view of risk should be avoided according to Nedaei et al. (2015). Risks should be viewed holistically (Nedaei et al., 2015). The foundation of ERM is that it is supposed to be value creating for firms, however, evidence of this relationship is limited. Kaplan and Mikes (2015) explain that despite the abundance of principles and guidelines risk management should not be considered a mature discipline and is still in its development phase. According to Kaplan and Mikes (2015), academics have suggested several contingency theories of ERM and have searched for specific circumstances that make for a specific appropriate risk management system for companies. However, studies that have tried to find the effectiveness of ERM have so far produced few significant results. Nedaei et al. (2015) explain that

organisational structure (decentralisation), size and enterprise resource planning might affect ERM practices of companies. Decentralisation is the allocation of responsibility and authority to managers and could allow the organisation's employees to be more autonomous and accountable as well. Moreover, a high level of decentralisation increases the need for coordination and control of the decentralised subunits. In this case, more sophisticated reports and control is thus required (Nedaei et al., 2015). Nedaei el al. (2015) also explain that larger organisations are subject to greater risk because of their more complex environments and therefore also require more efficient ERM methods. Lastly, the presence or planning of implementing an ERP system might affect the sophistication of ERM methods because of the large amount of data that an ERP system provides, as well as the risks that are inherent when implementing an ERP system. Kaplan and Mikes (2015) concludes, after a ten-year field-study in the area of ERM, that ERM will be most effective when "it matches the inherent nature and controllability of the different types of risk the organization faces" (2015, p. 40). They further conclude that "effective risk management "depends"; it is contingent on the organization's context and circumstances" (Kaplan & Mikes, 2015, p. 40).

A new testing ground for examining the effect of ERM were offered after the financial crisis in 2008 where the results were inconclusive and mixed, because firms ignore how frameworks are implemented by the organisation's employees and leadership, and are more focused on the adoption of a particular risk management framework (COSO's ERM). So to speak, the effectiveness of risk management depend on the people who coordinate, set out and contribute to risk management processes and less on the guiding framework (Tufano, 1996; Mikes, 2009; 2011). Also, risk management practices vary considerably across firms and even within an industry, which has been an emerging stream to understand risk management as a social and organisational practice according to Kaplan & Mikes (2015).

## 4.4 Relevance of the theoretical framework

Legislation and regulation has increased across the world in the area of internal control and reliability of companies' financial statements. Considering the spread of the increased legislation and regulation for publicly listed companies, together with the increased demand for companies to comply with shareholders and other stakeholders, stakeholder theory is highly relevant to

understand how companies should adapt to a changing reality in terms of whom it affects and is affected by. Furthermore, organisations are continuously trying to ensure that they are perceived as operating in accordance with the norms of society, according to Deegan and Unerman (2011, p. 323). Organisations try to ensure that their stakeholders perceive their activities as being legitimate. Society as a stakeholder is increasingly expecting businesses to expand its value creation, making legitimacy theory a highly relevant theory to use as a theoretical lens to understand the usage of the COSO framework to legitimise a company. Moreover, considering that all companies have different structures and that ERM should permeate the entire organisations, different ERM usage will occur within companies with different structures. Hence, contingency theory becomes relevant to evaluate the ERM of companies as well.

# 5. RESULT

*This chapter will cover the results of the multiple case study. The interviews will be collectively presented for each company and structured according to the four outlined areas of the Interview Guide as described in 2.4.3 Interview Guide. The results from the interviews are also complemented with results from the review of the annual reports and the IPO Prospectuses of the case companies.*

## 5.1 Company 1

### 5.1.1 Risk management on a general level

Company 1 is currently using COSO's framework and the catalyst for starting to use it was the IPO in 2014. The CFO explained that they started to implement the COSO framework six months after the IPO and the CFO is the one who is responsible for risk management within the company together with the auditing committee. Currently Company 1 is in the process of combining the operations and practices of different brands within the group considering that they created the consolidated group as late as in 2013. They are implementing COSO's framework step-by-step in the organisation, according to the CFO.

The CFO explained that the company in general wants to minimise risks. However, later on in the interview it becomes apparent that the company wants to minimise risks in terms of financial risk (for example foreign exchange risk) and internal control risk. Other classifications of risk were also mentioned during the interview, such as public relations risk and brand image risk. With that said, the CFO emphasised that in the end these risks affects the financials of the company and therefore should be considered. One of the primary reasons for wanting to minimise the financial risk of the company is because that they are a publicly listed company according to the CFO. In other privately owned companies hedging has not been as important since "larger hits" could be taken in the result according to the CFO. That is not possible to the same extent now being publicly listed. In general the CFO related his answers to the operations of the company and his duties of handling the financial risks.

Moreover, the CFO explained that Company 1 allows risks on a strategic level considering that they pursue growth both organically and through acquisitions. Hence, different risks are handled differently within the company. Financial and internal control risk should be minimised while strategic risk is allowed to be taken by the company. The Board of Directors lays the foundation of the amount of risk that is allowed to be taken by the company but the CFO also explained that the owners, customers and banks are significant stakeholders (emphasis on owners and customers) affecting the risk propensity of the company. The CFO explained that the ownership structure is currently changing with a few large shareholders changing into many small shareholders, which might affect the company's risk management.

On a general level the Financial Assistant is not aware of the risk management practices of the entire company but limited to the unit. Moreover, the Financial Assistant is not certain of who to contact regarding risk management, and explains that risk management have been pushed-back as not so important since there have been so much work with the IPO in general. However, the company has controls in place, indicated by the Financial Assistant later in the interview.

### 5.1.2 Internal Control practices

**Internal Environment**

The CFO explained that every component in the COSO framework is important for Company 1 and that the framework is effective. The CFO explained that you have to start with the environment, then you have a lot for free in terms of risk management. Currently Company 1 is working with risk assessment and that they are beginning to identify the existing control activities in the organisation and which ones they need to add. Thereafter information and monitoring will follow and secure that people are conscious about the risks. Information and monitoring are the difficult components of COSO's framework in the CFO's point of view. Because in this component of the framework you have to keep the risk management practices alive, that is the challenge. The CFO explained that it is easy to purchase a few consultant hours, but ingraining the practices in the company is the difficult part. The effectiveness of ingraining the practices in the company is what separates good and bad organisations according to the CFO.

**Risk Assessment and Control Activities**

In terms of their internal control practices the CFO explained that they have just finished the initial step of identifying significant risks for the company and that they are currently starting to map out existing control activities. Last year, in 2015, they set up workshops with top management and other groupings within the company to identify risks and the next step will be the internal auditing programme, which is put in place this year, in 2016. The internal auditing programme will primarily investigate the finance risk and internal control structure. Furthermore, the CFO explained that the company in general have good control activities but that they are informal and not documented. They are strong but informal due to the fact that they recently consolidated to a group and that the subsidiaries of the company previously had very strong owners in terms of the structure that they provided the companies. Now the structure is not provided for the subsidiaries to the same extent and it means that the formal risk management practices are not in place, meaning documentation etc. The old risk practices are still in place but there is a lack of documentation. In terms of its business operational side, the CFO of Company 1 explained that the security of the customers were important as well as that of other social aspects of its production when controlling its subsidiaries. The CFO continued to explain that new practices with COSO's framework and the internal auditors are implemented to get more control across the enterprise. Currently the risk management knowledge and thinking does not permeate the organisation but that is the next step of the process. Because currently they only have silo-thinking of risk in the organisation except for the case of their crisis management programme for their business operations. Company 1 had a crisis management plan if a security breach would occur in order to be able to stop production and solve the problem. This is supported by the Financial Assistant's knowledge of the risk management practices on a general level. The reasons why the risk management practices are so strong on a silo-basis of the business operations is because of their business area, where inspections are a common feature.

Furthermore, the CFO explained how they were doing so far in the improvement of the internal controls, using an illustration. Please view *Figure 5* below for a copy (adjusted) of the illustration. Since they started with the risk management practices, 6 months after the IPO, they have come halfway from informal to formal in their internal controls.

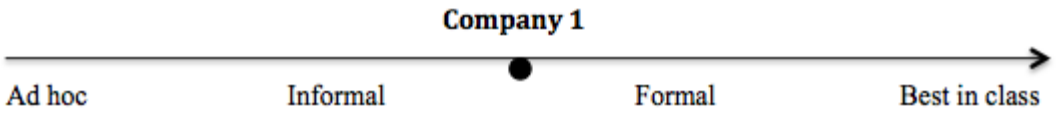


*Figure 5*: Company 1's internal control ranking

The CFO did not have any concrete examples of control activities, in terms of internal control, and explained that this is the phase that they are currently at in the usage of COSO's framework. Interesting enough was that they were starting with identifying control activities the day of the interview with an internal auditing team. Four points were going to be gone through by the internal auditors that day: governance (policy processes), production flow, financial risks and income controls. Next year there will be other points to go through for the internal auditors the CFO explained.

The CFO further explained that Company 1 wants to be formal in their practices and that the goal is to reach it in one to two years. After that they will start to manage and improve their practices. There are two reasons for wanting to become more formal in their control practices. One being control over risks and the other one being reduction of the direct cost to the company in regards to the auditing fees that have to be paid.

The Financial Assistant explained that the company is currently not that good regarding internal controls in the unit, and explains that there were no specific controls. Though, later in the interview, the Financial Assistant mentioned that there were job descriptions, process documents etc. The Financial Assistant believed that the company are starting to work with internal controls right now. Hence, the Financial Assistant supports the CFO when explained that this is where the company is in the current COSO usage. However, the Financial Assistant started at the company in 2014, and since then there have not been any significant improvements in the business unit. Though they have implemented some routines, deadlines etc. The Financial Assistant further explained that there are not as many external consultants working with the finance function as before (which is an improvement) and explained that the unit reports faults to the manager. Specific risks within the organisation has been brought up, though not extensively according to

the Financial Assistant. They currently act and handle the risks after faults occur. Risks are thus not handled preventively in this area.

**Information and Communication**

Information regarding processes, such as policy documents, can be found on the intranet as well as on billboards in the production facilities of the company, according to the CFO. Furthermore, meetings are held continuously so the company strives to have a continuous communication. Their internal control practices communication is limited though. The Financial Assistant explained that the communication in the organisation is good on a general level but not specifically in regards to risk.

**Monitoring**

Suppliers have to follow the supplier code of conduct and inspections are continuously made regarding the operations of the company according to the CFO. For example they have fire drills for risks on a regular basis, yearly, semi-annually etc. However, that is limited to the business operational side of the company. The internal control side is not at this stage yet. The later statement is supported by the Financial Assistant who explained that they do not have any continuously held meetings regarding faults and risks in terms of internal controls, but that is done on an ad-hoc basis.

### 5.1.3 ERM practices

In terms of risks on an enterprise level, Company 1 considers how crises, in terms of crises in their operations, affect the entire company and that they have a portfolio view of risks. They try to minimise these risks. Moreover, Company 1 has mapped out the risks of the organisation on a holistic level, creating a complete list of risks, according to the CFO. The strategic risks, in terms of expansion strategy and the risks inherent to running a business, are looked upon as through a risk appetite lens. Risk appetite in this respect is referred to as increase or decrease in shareholder value. The company has a pronounced expansion strategy in terms of organic growth as well as an acquisitive strategy. However, in terms of these risks, it appears as if they do not use the COSO framework compared to the internal control and business operations of the company.

Company 1 has experienced issues regarding their risk management on a strategic level in the organisation lately. They recently lost their CFO, last autumn. According to the current CFO, they would have needed a better back-up plan regarding this. The Financial Assistant explained that they have specific objectives and that they pursue these. Moreover, the customer is a stakeholder and affects the organisation heavily according to the Financial Assistant. Thus, it seems as if the general awareness and culture within the organisation is rigorous.

### 5.1.4 Implementation and usage of the COSO framework

There is a difficulty with risk management practices, that they are too formal, according to the CFO. It can be very expensive to mitigate very small risks and there are also inherent risks to running a company, which cannot be mitigated. Currently, Company 1 is in the phase of identifying control activities but the difficulties will come later when the practices has to be kept alive. Furthermore, it seems as if Company 1 uses COSO's framework on a step-by-step basis, moving to the next component of the COSO framework when the previous one is completed.

When asked if the new practices and COSO's framework has helped so far, the CFO responds that they do not know just yet.

### 5.1.5 Secondary Data

The secondary data gone through is the annual reports from the years leading up to the IPO as well as the annual reports after. Furthermore, the IPO Prospectus of Company 1 was investigated.

The company made its first reference to COSO's components in the IPO Prospectus and the first direct reference to specifically COSO came in the 2014 annual report and can also be found in the 2015 annual report.

## 5.2 Company 2

### 5.2.1 Risk management on a general level

Company 2 is currently using COSO's framework and the catalyst for starting to work more extensively with risk management and internal control was the IPO in 2015-2016. Prior to the IPO they had risk management practices but the organisation was characterised by a silo thinking towards risk, they did not have a holistic view of the risks of the organisation. In conjunction with the IPO the internal control function was set up. Furthermore, that is also the time when the Chief Audit Executive was recruited to the company. Hence, they started formalising the risk management and internal controls in conjunction with the IPO; structured analyses, strengthening existing controls and steering the group using frameworks. Previously risk management had been conducted informally. Currently, Company 2 is in the process of mapping out the risks in the organisation on a holistic level, according to the Chief Audit Executive.

The company has a complex structure which affects how risk management and control practices are executed in the organisation. Moreover, the company has completed several large acquisitions throughout the past years according to the Chief Audit Executive. The Chief Audit Executive explained that Company 2 acts within a risk appetite in terms of pursuing the objectives of the company and the risks inherent to the business. The company primarily uses COSO's framework in the financial function, the internal controller function, of the organisation. The Chief Audit Executive viewed it as an overarching guideline. The Chief Audit Executive mentioned that once the IPO was completed the ownership structure of the company changed.

### 5.2.2 Internal Control practices

**Internal Environment**

The Chief Audit Executive explained that due to the complexity of the organisation, risk management practices must be adapted to the organisational structure and business. For example the Chief Audit Executive is acting as an advisor as well as an auditor in order to be able to collaborate with the operational side of the company to set up risk management practices that do not hinder the business of the company. Moreover, the company works with co-sourcing when completing audits. For example, the company does not only audit their manufacturing processes

in Asia but brings in help from specialists in the firm to the manufacturers to also advise the companies on how they can improve operationally simultaneously as the audit occurs. Thus, the internal environment is characterised by a strong business perspective, even regarding risk management. Which also later becomes apparent considering that the Chief Audit Executive believes that the reason why they started with the new practices was also to be able to reduce costs. The Chief Audit Executive explained that the internal audit function within Company 2 should not be viewed as a police function within the company but as an advisor that has to understand the business practices of the company as well as audit the business, in order not to impair the business operations of the company. The Chief Audit Executive has the support from the top management of the company.

**Risk Assessment and Control Activities**

In terms of their operational controls and risk management practices, the Chief Audit Executive explained that Company 2 had strong controls prior to the IPO but that they had silo thinking. The Risk Assessment phase is where the company is currently at in terms of the COSO framework components. The Chief Audit Executive has had deep interviews with senior management within the firm and has been travelling to the different manufacturers of the firm, meeting managers. The Chief Audit Executive has collected information regarding risks and created a complete risk map with a holistic focus of risks within the company. The company has not yet mapped out controls in the organisation and has not created new controls to mitigate all of the risks that have been identified so far in the process. The Chief Audit Executive has scheduled to meet with the Auditing Committee of Company 2 to present the complete risk map. A meeting for a presentation to the board of directors has also been scheduled.

To illustrate the risks the Chief Audit Executive uses several risk frameworks, for example heat maps and risk matrices.

**Information and Communication**

In terms of information and communication it is important not to merely send information regarding risk management practices out in the organisation but spreading the message and making sure that people understands it and puts it into practice, according to the Chief Audit

Executive. Internal education is important to make this happen. For example, as an internal auditor, The Chief Audit Executive is travelling to the manufacturers of Company 2, meeting factory managers and making sure to understand their business reality before setting up risk management practices.

**Monitoring**

Company 2 had frequent inspections of the manufacturers of the company and made sure that all regulation and legalities were followed according to the Chief Audit Executive. This from a regulatory perspective, but also a business perspective so that they do not have to recall products. Moreover, in conjunction with the IPO they have started with formalised processes for risk assessment and also following up these risks. This was merely done informally prior to the IPO and not followed up to the same extent, as they now will be after the IPO.

### 5.2.3 ERM practices

On an enterprise level the company acted on the basis of their company's objectives and within a certain risk appetite. They did not try to minimise all risks, they evaluated their importance and the cost/benefit of mitigating the risks. The Chief Audit Executive specifically referenced shareholder value as a consideration in terms of risk appetite and the cost/benefit of mitigating risks. They had several risk functions in place before the IPO, however, the IPO was the catalyst for creating a holistic view of the risks and controls.

Company 2 does not use COSO's framework scrupulously in their risk management practices but as an overarching guideline. COSO's framework was mostly used in the finance organisation.

### 5.2.4 Implementation and usage of the COSO framework

One difficulty with implementing and formalising new and existing risk management practices in the company was the complex organisational structure as well as connecting it to the actual business practices of the company. Moreover, as previously stated, COSO's framework were not used scrupulously within the organisation on an enterprise level but was mostly used in the

finance organisation according to the Chief Audit Executive. Instead other frameworks and risk matrices were used to create a holistic view of risks.

According to the Chief Audit Executive the hard part is to get the risk management thinking ingrained in the culture.

#### 5.2.5 Secondary Data

The secondary data gone through is the annual reports from the years leading up to the IPO as well as the annual reports after. Furthermore, the IPO Prospectus of Company 2 was investigated.

The company made its first reference to COSO's components in their IPO Prospectus and the first direct reference to specifically COSO was made in their 2015 annual report.

### 5.3 Company 3

#### 5.3.1 Risk management on a general level

Company 3 is currently using COSO's framework and the catalyst for setting a new structure for internal control and risk management was the planned IPO in 2014 (the actual one occurred between 2015 to 2016). However, Company 3 had to postpone the IPO due to the external environment. The choice to improve the control practices came from top management and the board of directors, not a demand by the owners, and was introduced in the company due to increased regulation. Company 3 brought in external consultants and also created a board of directors in conjunction with the planned IPO in 2014. Moreover, they kept developing the new risk and control structure and reinforced it in the company despite the postponed IPO. Company 3 does not use COSO's framework as a direct tool in their risk management practices but more as an overarching guideline every year in top management meetings according to the CFO. Since their planned IPO in 2014 the company has performed risk evaluations every year through workshops where controls also have been investigated and set up, according to the CFO. Please view *Figure 6* below for an illustration of their risk map from 2014 and *Figure 7* below for an illustration of their risk map from 2015.

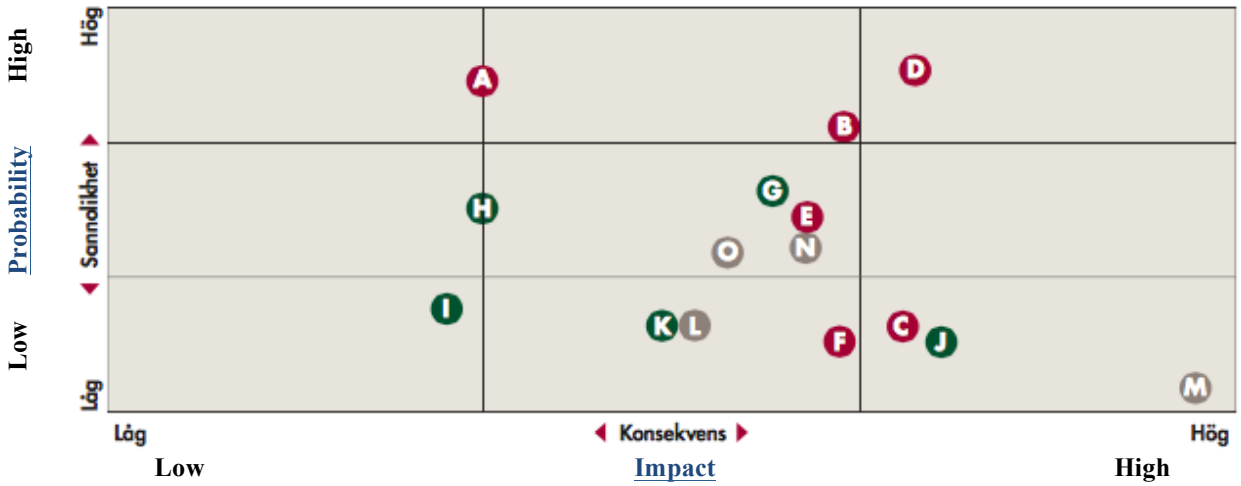


*Figure 6*: Company 3's 2014 risk map (2014 Annual Report)

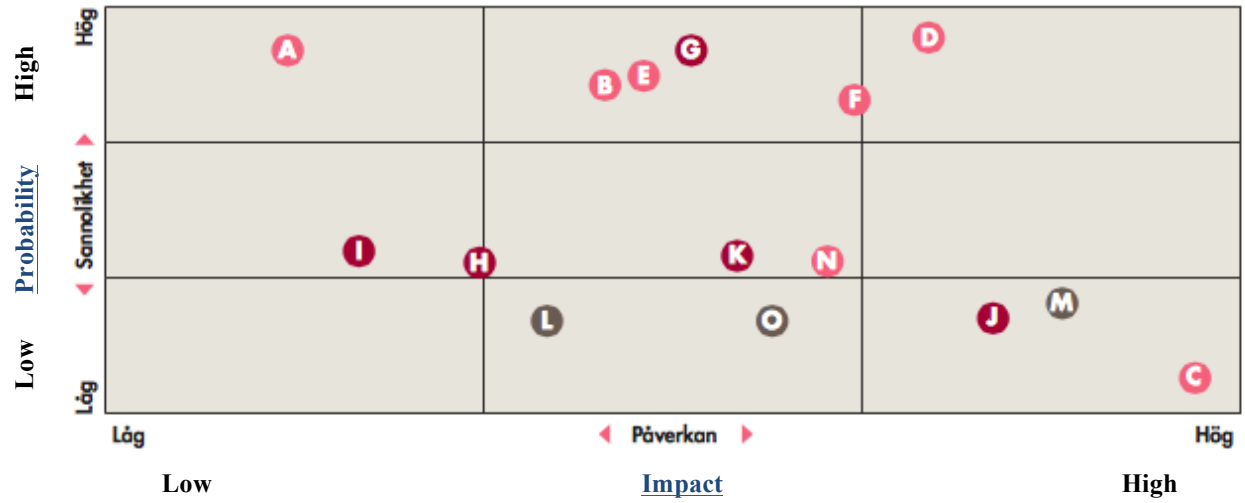


*Figure 7:* Company 3's 2015 risk map (2015 Annual Report)

In general the CFO explained that the company acts within a certain risk appetite, the company is using an acquisitive strategy and has acquired 30 companies since 2009. Most of the focus of risk management lies on the operations of the company and the risks inherent to their business. They are working directly towards consumers in a human service environment where the

appearance and customer service of the employees is crucial. The behaviour and treatment by employees is crucial in their line of business. Furthermore, their line of business is regulated and under scrutiny by organisations which frequently performs inspections of facilities, processes etc. Company 3 is acting in a political reality, according to the CFO.

The CFO explained that the ownership structure is changing slightly due to the IPO but that there is still a majority shareholder within the company. However, two large new owners are coming to the table and probably want seats on the board of directors. The CFO focused his interview on the risk management practices of the business operations of the company in general.

The Group Financial Controller of Company 3 does not utilise COSO's framework scrupulously but on an overarching level to identify risks. Worth noting though is that Group Financial Controller has recently started working for Company 3 and has just started identifying risks within the financial reporting processes. The Group Financial Controller is aware of the objectives of Company 3 and aims to create a holistic view of the processes within the company in the future so that everyone is aware of the challenges throughout the processes. Furthermore, the Group Financial Controller, much like the CFO, explained that all risks cannot be minimised.

### 5.3.2 Internal Control practices

**Internal Environment**

Due to the sensitivity of the company's operations, a proper culture is of paramount for Company 3 and they have a value-based organisational culture, according to the CFO. This explanation was further reinforced by the researchers noticing explicit stories, showing signs of a strong value-based culture, displayed in the company headquarters on digital billboards. Moreover the company tries to create what the CFO calls a "positive fault culture", meaning that people should be able to report to management if something is not done properly or if a fault has occurred, it is important to nurture that behaviour the CFO explained.

Moreover, the board of directors that the company established in 2014 included a well-renowned professional within auditing and with knowledge of COSO's framework. The board of directors have oversight over the risk management practices of the company.

The Group Financial Controller has support from top management and explains that top management is interested in the potential of errors occurring in the processes. Furthermore, the Group Financial Controller explained that it is important to get everyone involved in the project of risk management and also create a culture where people act the same way regarding risks. One of the main points was to create flow charts instead of using text documents to do this. Everyone in the company does not hold a business degree and as such flow charts can help visualise the processes within the company for everyone according to Group Financial Controller.

**Risk Assessment and Control Activities**

In terms of Company 3's internal control practices, the CFO explained that they have always had a strong view of the operational side of the risks but in 2014 when the external consultants reviewed the company it opened the company's eyes for risks in the financial reporting. Company 3 does not have an internal auditing function since the CFO is strongly against such a function and believes that it is not sufficient for evaluating their line of business operations. It cannot be used to certify the quality of the company. It does not add value.

In 2014, Company 3 set up workshops with top management to identify and review the risks of the company. They identified several risks and also set up controls for these risks. A specific example regarding the political risks that the company is subject to was brought up. The CFO explained that a risk was identified and also a control for this risk, Company 3 hired a lobbyist. However, the CFO emphasise that risks are not purely bad, they are also opportunities. The acquisitive strategy of the company is an example of this, since the strategy has significant risks inherent to it. The risks being for example the risks when growing larger and keeping track of a larger organisation as well as other companies having a different code of conduct to customers etc. according to the CFO. However, Company 3 evaluates these risks when finding acquisition targets.

Specific control activities on the business operational side of the company was mentioned, both internal controls as well as external controls. These controls were for example inspections of the facilities and processes within the operations. The inspections were both announced and

unannounced from both inspection parties. Moreover, the company's financial reporting controls are solid with for example routines as well as with their usage of automated controls according to the CFO. The company specifically have control systems for their operations in terms of a financial control system and a quality control system where the financial control system works as an indicator for inappropriate operations within the company and a quality control system where they continuously perform inspections to facilities etc.

The Group Financial Controller is currently in the process of identifying risks within the financial reporting processes of the company and explained that this is where the company currently is at in the COSO framework, even though they do not use it scrupulously. Furthermore, the Group Financial Controller viewed risks as "red" or "green" (red being more important to mitigate). Hence, much like the CFO, the Group Financial Controller regards risks as risks within a specific risk appetite and is trying to mitigate the red risks. The Group Financial Controller explained that one task right now is to make sure that the entire group use the same processes and standards in the financial reporting, because they have expanded aggressively the past years. The Group Financial Controller also stated that it is not absolutely certain that everyone is performing valuations the same way, even though they probably are. That is why the Group Financial Controller wants to introduce one standard across the entire group, however, that standard should be able to have deviations in order not to be too static. Moreover, the Group Financial Controller also supports the CFO's statement of automated controls in the interview, explaining that this is an area, which should be developed further.

**Information and Communication**

In terms of information and communication, the employees can gain access to information, policies, procedures etc. through the intranet. Moreover, the company have workplace meetings, management meetings and they also try to provide information to iPhones, iPads etc. Furthermore, considering that Company 3 works with people and has practices with social interactions, descriptions on paper is not sufficient. That is why the meetings and collaborations between colleagues take place. Furthermore, as has been explained in the *Internal Environment*, the company also displays their values and stories on digital billboards in the headquarters.

The Group Financial Controller explained that the employees in the finance department have access to process maps and routine descriptions in their line of work.

**Monitoring**

Company 3 frequently issued inspections to the facilities of its operations and followed up so that the practices within the firm were adequate, according to the CFO. Furthermore, since they started assessing the risks within the firm in 2014 they followed them up with a review in 2015 where some of the risks had been realised, and thus did not qualify as risks again.

### 5.3.3 ERM practices

In terms of risks on an enterprise level, Company 3 does not consider risks as simply bad, but as opportunities as well. Thus, they act within a specific risk appetite, risk/reward reality according to the CFO. The company has an acquisitive strategy for example, having acquired 30 companies since 2009. Moreover, they work preventively to identify risks within the company before they occur. However, in terms of these risks, it appears as if they do not specifically use COSO's framework. Lastly, they also view risks holistically.

Company 3 works proactively with identifying risks and they are aiming towards gaining a holistic view of risk management. Also, the Group Financial Controller is aware of company objectives.

### 5.3.4 Implementation and usage of the COSO framework

One issue with risk frameworks according to the CFO is that one can limit oneself with too much focus on risk thinking in an organisation in terms of using a specific framework. Company 3 takes an overarching guideline approach to the COSO framework. The difficulties in the usage so far for the company have been that of evaluating the identified risks within the organisation according to the CFO.

Despite the company’s aggressive acquisition strategy they have not experienced culture clashes with the acquired companies. They analyse these aspects when acquiring the companies and

make sure that every company have the same norms and values according to the CFO. Furthermore, they work with the control practices through gradual implementation.

It seems as if the company is not implementing the COSO framework as their risk management practices but are using it as an overarching guideline. For example they have identified and controlled certain risks but the financial reporting risk is just now being mapped out. They recently hired the Group Financial Controller who is responsible for the internal controls.

In terms of usage of the framework the Group Financial Controller does not use the framework scrupulously in the risk management work. The COSO framework is mostly used as an "external tool" to view practices once they have been identified, according to the Group Financial Controller. One of the main difficulties going forward according to the Group Financial Controller will be to create standardised processes and making sure that everyone performs tasks similarly, they probably do this in most cases but processes should be set up. This is especially hard considering how fast they have been growing lately, with so many acquisitions. Currently, the company is in the Risk Assessment component in the COSO framework according to the Group Financial Controller.

### 5.3.5 Secondary Data

The secondary data gone through is the annual reports from the years leading up to the IPO as well as the annual reports after. Furthermore, the IPO Prospectus of Company 3 was investigated.

The company made its first reference to COSO's components in their 2014 annual report (2014 was the year that the company initially tried to complete their IPO) and references to the components can also be found in the IPO Prospectus as well as in their 2015 annual report.

# 6. ANALYSIS

*The results from the interviews with the three case companies will be analysed using the theoretical framework throughout this chapter and a summary of the findings will also be concluded at the end.*

## 6.1 Risk management on a general level

All three case companies in the study increased their internal control and risk management practices in conjunction with the IPO, which is in accordance with Wendt's (2016) explanations. All of the companies had operational risk management thinking and practices prior to the IPO, however, the IPO was the catalyst for formalising the practices on a group level to a large extent. It is clear that the companies had a silo thinking of risks and control within the organisations before the IPOs took place. The secondary data also supports Wendt's (2016) viewpoint, clearly indicating that COSO's framework were implemented in conjunction with the IPOs of the companies in this thesis, whether that is in the IPO Prospectus or in the annual report if the IPO was postponed.

Wendt (2016) explained that increased regulation when becoming a publicly listed company is the catalyst for the introduction of formal processes, which is also in line with our findings. However, two companies also mentioned the financial and business perspectives of implementing COSO's framework. Company 1 and Company 2 wanted to reduce the costs by implementing the framework. Hence, increased regulation is not the sole purpose why companies implement increased risk management when publicly listing.

Two companies, Company 1 and Company 3, had several stakeholders affecting risk management. The most important stakeholders of Company 1 were the owners, customers and banks and Company 1 needed to minimise their risk in their business operations due to its customers. Company 3 also made references to their customers as a stakeholder, explaining that providing a proper service to the customers is a reason why they have a lot of risk management in their operations. Hence, the companies' risk management practices can be viewed from a stakeholder theory perspective where the stakeholders of the firms are affecting the practices of

risk management of the firms. However, this is not only apparent in terms of the business operations risk but also for the strategic risk and financial reporting risk of the firms. This became obvious when the managers explained that their ownership structure changes now after the IPO and that the new owners can create changes regarding the risk management of the firms. For example Company 1 explained that its owners affect their risk propensity and that after the IPO it has become important to minimise the financial risk. As a private company they could take larger hits in the result and did not have to hedge to the same extent. Furthermore, this highlights the salience of the shareholders as a stakeholder, in accordance with Mitchell et al.'s (1997) view of the varying importance of stakeholders to management and that stakeholders' salience can change. From the shareholders' perspectives they expect to get a say in the risk management practices since they want to "safeguard their asset-specific investments in the firm", as Hill and Jones explain about large stakeholders (1992, p. 133-134). The view that the customers affect the risk management practices to creating an aspect of minimising risks for Company 1 is interesting. It illustrates that an economic measure of value for them is not the single consideration of value. Security creates a value in itself for them and broadens the managers perception of value creation, as Harrison and Wicks (2013) explain.

The findings are is also in line with Deegan´s and Unerman's (2011) view, which explains that in recent years significant changes in public opinion has emerged. Heightened social expectations are emerging and in order for society to perceive a company as successful it has to be attentive to human, environmental and other social consequences of its activities. Company 1 explained that not only the security of the customers were important but also that other social aspects of its production was important for the company when controlling its subsidiaries.

Furthermore, Deegan & Unerman (2011) explain that society as a stakeholder is increasingly expecting businesses to expand its value creation and that failure to comply with the expectations may result in imposed sanctions in the form of legal restrictions on the operations or resources of the company in question, or an impaired demand of the products or services of a company by its consumers. Company 1 had a crisis management plan if a security breach would occur in order to mitigate the negative impact in terms of impaired demand and legal restrictions. Company 1 can also be considered to use reputation risk management in regards to their crisis management

plan, which is a legitimation strategy used to secure their resources for future profits as Deegan and Unerman (2011) explains. Company 3 hired a lobbyist to mitigate the political risk the firm was facing which can also be considered to be a legitimation strategy considering that it is performed to maintain the legitimacy of the firm. This action and legitimation strategies overall are connected to Company 1's and Company 3's risk management practices. Hence, legitimacy theory is a great tool to analyse the risk management of the two companies.

## 6.2 Internal Control practices

In terms of the companies' internal control practices and their usage of the COSO framework they are all working within the same component of COSO's framework, namely in the Risk Assessment component (however, as will be discussed in the *6.4 Implementation and usage of the COSO framework* the three companies use COSO's framework differently), this despite the fact that Company 1 publicly listed as early as in 2014 and Company 3 as late as between the end of 2015 to the middle 2016. This indicates that it takes a lot of time and effort to move beyond the Risk Assessment phase to controlling the identified risks. However, Company 3 had been able to mitigate some risks identified in the Risk Assessment phase but can still be considered to be in the Risk Assessment component, for example since the Group Financial Controller is currently getting started mapping out the financial reporting risks of the firm. However, interview persons within all three firms thought ingraining the control activities in the culture of the organisation and making sure that the employees perform them was going to be the most difficult phase. As the CFO of Company 1 explained, it is easy to purchase a few consultant hours, but ingraining it in the company is the more difficult part. Thus, the companies might still stand in front of their biggest challenge yet in terms of implementing and using the COSO framework.

Another reason why all companies currently are in the same phase in the usage of the COSO framework, despite having significantly different IPO dates, might be because that the owners prior to the IPO possibly could have differed in sophistication and experience. The previous owners might have prepared the companies for an IPO differently. This does not seem likely though considering that the owners prior to the public listings of the firms were not too

dissimilar. All three companies had private equity funds (sophisticated investors that are used to list (IPO) their portfolio companies on stock markets) as owners prior to the IPOs. Hence, the sophistication and experience of prior owners in IPOs should not impact the result significantly.

## 6.3 ERM practices

All three companies use the COSO framework differently within their organisations. Furthermore, it seems as if the companies regard the Internal Environment component of the COSO framework on an enterprise level. For example, Company 3 explained the importance of creating a value-based organisational culture across the firm and a "positive fault culture". Moreover, Company 2's culture seems to be highly focused on the business perspective of the company. There were no strong indications that Company 1 had a single omnipresent culture among its employees, though there was a strong risk management focus within the subsidiaries. Moreover, all interviewees seem to have the support from top management, the board of directors or their supervisors. However, with the internal environment as an exception, it seems as the COSO framework are mostly used for handling financial reporting risks and setting up controls in this respect, not for handling risk on a strategic level. Neither case company showed any significant signs of using the COSO framework for handling strategic risk to a large extent. The companies instead use their own frameworks, models and illustrations internally for handling risks. Company 1 had its own figure for explaining their internal control ranking (please view *Result*, *Figure 5*). Company 2 used various frameworks models and Company 3 showed their frameworks from their annual reports (please view *Result, Figure 6* and *Figure 7*). However, it becomes apparent that all companies use COSO's framework at least as an overarching guideline since all companies discuss it during meetings with top management and/or with the board of directors.

With that said, not directly utilising the COSO framework for all aspects of risk management and merely using it as an overarching guideline, does not exclude that they use ERM. Comparing the risk management of the companies to the definition of COSO it becomes apparent that they use ERM within the organisations. COSO's (2004, p. 2) definition is stated below and the underlined

bullet points represent that the companies are currently considering this perspective in their risk management:

- "A process, ongoing and flowing through an entity
  Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories"

All companies explain that they increased the formality of their risk management (in terms of formally documented procedures etc.) in conjunction with the IPO. They went from a silo-based approach of risks to viewing risks on a holistic level, aiming to map out all risks and controls in the organisations. All companies had identified a complete list of risks that could occur and affect the organisation. However, only Company 3 explicitly stated that they had acted preventively to mitigate these risks, having hired a lobbyist to reduce the political risk. A holistic view of risks is one of the cornerstones of ERM according to Nedaei et al. (2015). Moreover, COSO explains in their definition of ERM that companies should take an "entity-level portfolio view of risk" that is on-going, which is what the companies currently are doing. Hence, the IPO of the firms seems to be a catalyst for implementing ERM in this respect.

Moreover, all companies consider risks from a risk appetite perspective in terms of the risks on a strategic level and regarding the companies' objectives. Company 1 aimed at minimising risks in their operations and in terms of foreign exchange rates etc. but not in terms of strategy, considering that they have an acquisitive strategy with inherent risks. The other two companies also had acquisitive strategies viewing risks as opportunities and benefits in terms of risks for shareholder value and also considered the objectives of the firm as a whole. Hence, a risk appetite view of risks could be found in all three companies. However, there was no indication

that the risk appetite view of risks was introduced in conjunction with the IPO. It seems as if the risk appetite view of risks was already held within the firms prior to the IPO, especially considering the acquisitive strategies of the firms.
In addition, it seems that all companies' board of directors were provided the risk management information of the firms. In Company 1 the CFO explained that the board of directors lays the foundation of the amount of risk that is allowed to be taken by the company. Moreover, the decision to implement COSO's framework in the first place for Company 3 was decided by the board of directors and the risk maps of the company can be found in their annual reports, which the board of directors have approved. Lastly, the Chief Audit Executive of Company 2 has scheduled meetings with the board of directors regarding the risk management of the company.

An ERM perspective is taken by the firms in regards to most of the aspects brought up by COSO (2004) in its definition of ERM, except for that the ERM thinking does not permeate the entire organisations. COSO states that ERM is supposed to be " flowing through an entity" and that it is supposed to be "effected by people at every level of an organization" etc., this is not the case (2004, p.2). The companies are still in the Risk Assessment phase of the COSO framework and have not yet mitigated all risks identified in the organisations. For example, Company 1 and Company 2 were currently formalising the risk management within their subsidiaries but could not be considered to have a permeating risk management according to the definition of COSO (2004).

## 6.4 Implementation and usage of the framework

The three companies use the COSO framework differently in their organisations. Company 1 seems to be the only company that use COSO's framework scrupulously, on a step-by-step basis. Company 2 mostly use it in the finance function and the Chief Audit Executive uses it as an overarching guideline. That is also the Case of Company 3, which is also the only company not using internal auditors in the organisation. The reason why two of the companies do not use COSO's framework scrupulously can be tied to the organisational structures of the firms and their business practices. The Chief Audit Executive of Company 2 explained that one difficulty when implementing and formalising new and existing risk management practices in the company

was the complex organisational structure and their operations. Moreover, the CFO of Company 3 explained that you could limit yourself with too much focus on risk thinking in terms of a framework. Additionally, the CFO explained that the reason that they did not have an internal auditor was because that it was not suitable in their line of business. Hence, the usage of COSO's framework seems to be contingent upon the business and the organisational structure and the findings is also in line with Donaldson's (2001) thoughts on contingency theory.

According to Donaldson (2001) contingencies that affect companies' actions include the environment, organisational size and organisational strategy. Moreover, in terms of contingency theory, specifically regarding ERM, it is in line with Nedaei et al.'s (2015) view that companies should manage risk in accordance with their characteristics, the characteristics being size and nature of operations. Additionally, Nedaei et al. (2015) explain that activities that further increase the complexity of organisations are mergers, deregulation etc. and that risks should be viewed on a holistic level. All three case companies have acquisitive strategies and that has affected their organisations in terms of increased risk. Several respondents specifically mentioned this. The Group Financial Controller in Company 2 explained that the many acquisitions have increased the complexity of the financial reporting, complexity in terms of making sure that everyone does things the same way. Furthermore, it is relevant for the case companies to not use a specific risk framework scrupulously in their risk management considering that they want to maximise their performance. Donaldson (2001) explain that considering that higher suitability of the organisation's characteristics with its contingencies leads to higher performance, organisations will seek to be suitable to its contingencies. Kaplan and Mikes (2015) also supports this view specifically regarding ERM of companies and explain that ERM will be most effective when "it matches the inherent nature and controllability of the different types of risk the organization faces" (2015, p. 40). Kaplan and Mikes further conclude that "effective risk management "depends"; it is contingent on the organisation's context and circumstances" (Kaplan & Mikes, 2015, p. 40). Thus, it makes sense for Company 2 and Company 3 to have adopted risk management practices to their specific context and circumstances.

Moreover, two companies had specific circumstances to adapt to. Company 3 had to consider its political reality and Company 1 had to consider their customers' and other social aspects in its risk management. Hence, legitimation strategies were used in the risk management by both of the companies. In addition, the usage of COSO's framework could be a part of the companies' overall legitimation strategy. Because, Deegan and Unerman (2011) explain that companies can be provided legitimacy by association if they collaborate with legitimate organisations. COSO can be considered a legitimate organisation since its framework are recommended by the SEC in the US and are considered the most established framework in the areas of internal control and ERM according to the Institute of Internal Auditors (2008). When becoming publicly listed, companies face more scrutiny from investors and regulators, and the regulators are supposed to protect society. If the companies state that they use COSO's framework it can legitimise them in the view of investors and regulators. An aspect strengthening this argument is that Company 3 is merely using COSO's framework as an overarching guideline. However, as has been explained, this is due to the contingencies the companies face which should affect their ERM if they want to have an effective ERM, according to Kaplan and Mikes (2015). Moreover, what contradicts the viewpoint that COSO's framework is merely used to legitimise the company, is that the three case companies' purpose for formalising their controls is not limited regulation, but also includes the direct business and financial benefits of formalising their controls according to the companies. Additionally, Company 3 did not use an internal audit function, and did not plan to implement one either, which is in opposition to the advocacy of the function by the Code (2015), which states that companies either should have an internal audit function, or explain its decision for not having it. Using an internal audit function could have been used to legitimise the company's practices further. Lastly, Company 3 also set up a board of directors with specific COSO framework knowledge in conjunction with its planned IPO and the company also continued to use COSO's framework despite the deferment of the IPO. Hence, the risk management of Company 1 and Company 3 involves legitimation strategies, but their usage of COSO's framework and their risk management on a general level should not be considered to be an entire legitimation strategy.

According to Lindblom (1993, recited in Deegan & Unerman, 2011) companies can use their annual reports to execute various legitimation strategies. The secondary data does not indicate

that the companies use COSO's framework as a hollow legitimation strategy, hollow as in not actually changing the practices of the company, considering that COSO is not referenced before the companies actually started to formalise their internal control and risk management. Company 1 started working according to COSO's framework six months after the IPO according to the CFO. In the IPO Prospectus, Company 1 does not specifically mention COSO but only its components. The first reference to COSO was made in the 2014 annual report and considering that they started working with COSO's framework 6 months after the IPO the secondary data confirms the findings from the interview with the CFO. Thus, COSO's framework, and the company's risk management do not seem to be used as a hollow legitimation strategy since they actually started to use COSO's framework, even though the control activities section can be considered a bit too optimistic, compared to the result from the interview with the Financial Assistant of Company 1. Company 3 started using COSO's framework in conjunction with the planned IPO in 2014 according to the CFO and the first reference to COSO's components can be found in their 2014 annual report. Moreover, the CFO stated that they continued to use COSO's framework, which is supported by the secondary data. Overall the annual reports and IPO Prospectuses seem to be reflecting the reality of the companies' practices. Taking all sections above that analyses the risk management from a legitimacy theory perspective into consideration, all companies seem to use the legitimacy strategy of: Educate and inform the stakeholders of actual changes of the firm's activities and performance which are in line with society's expectations, but the usage of COSO's framework in itself is not in its entirety used for legitimation but also for reducing costs.

## 6.5 Summary of the insights

The analysis provides several insights into newly publicly listed companies' usage of the COSO framework. A summary of the findings can be found in bullet points below.

**Risk management on a general level**

- IPOs seems to be a catalyst for starting to use the COSO framework, introducing more formalised control processes and forming a holistic view of a company's risks.

- Newly publicly listed companies use the COSO framework to respond to regulation as well as to be able to reduce costs.
- A newly publicly listed company's stakeholders affect their overall risk appetite and their risk management.
- The salience of stakeholders shift in conjunction with an IPO considering that the ownership structure changes for a newly publicly listed company.

**Internal Control practices**

- It is difficult for newly publicly listed companies to move beyond the Risk Assessment component of the COSO framework.
- Ingraining the control activities in the culture of the organisation and making sure that the employees perform the control activities will become the most difficult phase of risk management for publicly listed companies.

**ERM practices**

- The COSO framework is primarily used for financial reporting for newly publicly listed companies.
- Even though newly publicly listed companies do not specifically use the COSO framework to manage risk on a strategic enterprise level, they view risks from an ERM perspective.

**Implementation and usage of the framework**

- Newly publicly listed companies use the COSO framework differently, either scrupulously on a step-by-step basis or more as an overarching guideline.
- Risk management of newly publicly listed companies involves legitimation strategies but the usage of the COSO framework should not in its entirety be considered a legitimation strategy considering that it is also used to reduce costs.

A discussion of how companies use the COSO framework and the experienced difficulties when doing so will be held in the next chapter in order to fulfil the purpose of the thesis.

# 7. DISCUSSION & ENDING REMARKS

## 7.1 ERM usage is contingent upon context and circumstances

In the aftermath of accounting scandals and financial crises companies are facing increased regulation and legislation from governments aiming to protect public interest. In order to respond to the new environment with increased regulation and legislation, in terms of specifically corporate governance and financial reporting, companies have started to use risk management frameworks such as COSO's well-established framework to ensure the creation of stakeholder value. However, COSO's framework is merely a way of working when handling risks within an organisation, not a certification that the risk management is adequate and that stakeholder value will be created. Furthermore, as we have seen in this thesis, newly publicly listed companies use COSO's framework differently, contingent upon its business context and its circumstances. Of the three case companies, Company 1 was the organisation that used the COSO framework the most scrupulously on a step-by-step basis, while Company 2 and Company 3 used it more as an overarching guideline. However, despite this, Company 1 cannot be considered to have a superior risk management or superior financial reporting controlling procedures. Hence, COSO's framework merely provides a way of working with risk management for companies and demanding that companies use the COSO framework is in itself not sufficient for controlling the companies from risks. What matters, is what a company actually achieves in terms of risk management by utilising the framework.

## 7.2 Moving beyond the Risk Assessment component of COSO takes time

All three case companies were approximately in the same phase of their risk management processes in terms of which COSO component they had completed, specifically the Risk Assessment component. This despite the fact that they used COSO's framework differently within their organisations as well as having publicly listed at different times. Moreover, all companies explained that the most difficult phase would be to ingrain the new risk management practices in the company and making sure that the employees actually complete them. The CFO of Company 1 explained that it is easy to purchase a few consultant hours, but ingraining the practices in the company is the difficult part. Additionally, the CFO explained that the effectiveness of ingraining the practices in the company is what separates good and bad

organisations. This illustrates the difficulties of executing planned strategies for organisations. Simons (2013) advocates a greater focus on strategy execution in Business Schools. Moreover, Simons (2010) explains that strategy execution requires tough and uncomfortable choices based on simple logic and clear principle but that one often lose sight of this simple logic and clear principle in the complexity and by the techniques that consultants and the business press advocate. Hence, viewing the usage of COSO's framework within newly publicly listed firms as an example, illustrates the difficulties of executing strategies for an organisation. Moreover, none of the case companies had managed to create an ERM view across the entire enterprise. Changing the behaviour of an organisation and making sure that ERM permeates the entire organisation seems to take longer than the investigated years since the IPOs in this study. Employees are often unwilling to commit to organisational change since it disrupts their existing routines and social relationships, which they have relied upon to complete their work tasks according to several academics (Beer, Eisenstat, & Spector, 1990; Strebel, 1996, recited in Shin, 2012). Moreover, previous research shows that planned organisational change is a fatiguing process for employees that is long and emotionally intense. Hence, it comes as no surprise that it takes time for companies to mature its usage of the COSO framework and to enable ERM to become prevalent in the organisational culture.

As an ending remark to the discussion and the analysis of this thesis we would like to reiterate that COSO's framework provides a way of working with risk management for companies but should not be considered a certification for adequate risk management. Hence, demanding that companies use the framework is not a solution in itself to the trust issues that companies are facing, however, it does provide a guideline of how to formalise a company's risk management and work with risk on an enterprise level.

## 7.3. Conclusion

The thesis has developed previous knowledge of how ERM is used by Swedish publicly listed companies by investigating the ERM of recently publicly listed Swedish companies. Companies use COSO's framework differently, contingent upon its business context and its circumstances

and the difficult phase of ERM will be for companies to ingrain the new risk management practices in the company and making sure that the employees actually complete them.

## 7.4 Further studies

This thesis has laid a foundation for future research of how companies that want to formalise their risk management use COSO's framework to create adequate risk management within their organisations. The thesis indicates that an IPO works as a catalyst for creating formalised risk management across a firm on a holistic level. However, the study has been rather limited as is described in *2.7 Limitations,* so in order to be able to generalise the result a larger sample of firms should be investigated. Hence, a suggestion for a further study is to conduct a survey study aiming at generalising the conclusions of this study in order to provide companies, legislators and investors with an indication of how far the formal risk management of a company can be expected to have come within a specific time range after an IPO.

An additional suggestion for further studies is to deepen the investigation into the risk management of companies, interviewing multiple divisions and hierarchical levels within the firm in order to gain a deeper understanding and a holistic view of the risk management practices of organisations. Moreover, it would be interesting to conduct this study longitudinally, following firms from the implementation decision of the COSO framework to the mature usage of ERM. This to view the evolution as well as revolution of the risk management practices within firms and document the differences of risk management over time.

We would also like to issue a caveat to future research that will be using qualitative semi-structured interviews to investigate risk management within organisations. It is important to consider which information that is required to be obtained when choosing the respondents, because it became apparent during this study that depending on who you interview in the organisation, the respondents relate and bring up different perspectives of risk management. CFOs elaborate on risk in the business operations of the company while the finance department mostly speak about risks in terms of in their own unit. Hence, in order to obtain a holistic view of ERM, multiple divisions and hierarchical levels should be interviewed.

# 8. REFERENCES

Andersen, J.T. & Winther Schrøder, P. (2010). Strategic Risk Management Practice: How to Deal Effectively with Major Corporate Exposures. Cambridge University Press. Available online: https://books.google.se/books?id=xFly_CoerqwC&pg=PA124&lpg=PA124&dq=hazard,+operational,+financial+strategic+risks&source=bl&ots=wvwGIYeIgU&sig=eZHKjitF5qRqDY2lRFviT_tSC9Y&hl=en&sa=X&ved=0ahUKEwjxhr6M8dbLAhWpd5oKHfNYCN04ChDoAQghMAE#v=onepage&q=hazard&f=false Accessed, [2016-03-23]

BaxterBruce. (2013). Enterprise Risk Management: The Challenges and Benefits of Implementing ERM. Available online: http://www.baxterbruce.com/wp-content/uploads/2013/05/ERM-The-Challenges-and-Benefits-of-Implementing-ERM.pdf Accessed, [2016-03-28]

Beer, M., Eisenstat, R. A., & Spector, B. (1990). Why change programs don't produce change. *Harvard Business Review,* 68(6): pp. 158-166.

Berg, P. & Skoogh, C. (2012). Enterprise Risk Management: Hur använder svenska företag ERM. Göteborgs Universitet. Available online: https://gupea.ub.gu.se/bitstream/2077/29634/1/gupea_2077_29634_1.pdf

Bonnefond, J. & Lounkokobi, K. (2007). Sarbanes-Oxley section 404 Impacts on European companies. Available online: https://www.diva-portal.org/smash/get/diva2:140533/FULLTEXT01.pdf Accessed, [2016-03-24]

Bryman, A. & Bell, E. (2011). Business research methods, (3rd Ed.). New York: Oxford University Press.

Bylund, J. & Haggren, C. (2006). Svensk Kod för Bolagsstyrning: En förtroendeskapande åtgärd? Södertörns Högskola. http://www.diva-portal.org/smash/get/diva2:16185/FULLTEXT01.pdf Accessed, [2016-03-24]

COSO. (2003). Available online: http://www.coso.org/documents/internal%20control-integrated%20framework.pdf Accessed, [2016-03-29]

COSO. (2004). Available online: http://www.coso.org/documents/coso_erm_executivesummary.pdf Accessed, [2016-03-28]

COSO. (2010). FAQs for COSO's Enterprise Risk Management: Integrated Framework. Available online: http://www.coso.org/erm-faqs.htm Accessed, [2016-04-14]

COSO. (2011). Embracing Enterprise Risk Management: Practical Approaches for Getting Started. Available online: http://www.coso.org/documents/EmbracingERM-GettingStartedforWebPostingDec110_000.pdf Accessed, [2016-04-14]

COSO. (2013). COSO Internal Control-Integrated Framework - Frequently Asked Questions. Available online: http://www.coso.org/documents/coso%20faqs%20may%202013%20branded.pdf Accessed, [2016-04-01]

COSO. (2015). COSO at 30 Years: April 16, 2015. Available online: http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/programs/sechistorical-041615-transcript.pdf Accessed, [2016-03-24]§

COSO. (2016). Available online: http://www.coso.org/aboutus.htm Accessed, [2016-03-24]

Damodaran, A. (2008). Strategic Risk Taking: A Framework for Risk Management. Pearson Prentice Hall. Available online:

https://books.google.se/books?id=TJ0dnfed0_wC&pg=PA3&lpg=PA3&dq=Risk+is+part+of+every+human+endeavor.+From+the+moment+we+get+up+in+the+morning&source=bl&ots=9Y_YH2E89R&sig=-KXFyOSrJwKbMlJA_Klpre8mlaA&hl=en&sa=X&ved=0ahUKEwjO-b3H6dbLAhUmb5oKHQt3ANIQ6AEIGzAA#v=onepage&q=Risk%20is%20part%20of%20every%20human%20endeavor.%20From%20the%20moment%20we%20get%20up%20in%20the%20morning&f=false Accessed, [2016-03-23]

Deegan, C. & Unerman, J. (2011). Financial Accounting Theory. McGrawHill. 2nd European Edition.

Donaldson, L. (2001). The Contingency Theory of Organizations. Foundations for Organizational Science. *Sage Publications, Inc.* California

Dionne, G. (2013). Risk Management: History, Definition and Critique. Interuniversity Research Centre on Enterprise Networks, Logistics and Transportation (CIRRELT). Available online: https://www.cirrelt.ca/DocumentsTravail/CIRRELT-2013-17.pdf Accessed, [2016-03-28]

Dornberger, K., Oberlehner, S. & Zadrazil, N. (2014). Challenges in Implementing Enterprise risk Management. *ACRN Journal of Finance and Risk Perspectives*. Vol. 3(3), pp. 1-14. Available online: http://www.acrn-journals.eu/resources/jfrp201403a.pdf Accessed, [2016-03-28]

EY. (2012). The Sarbanes-Oxley Act at 10: Enhancing the reliability of financial reporting and audit quality. Available online: http://www.ey.com/Publication/vwLUAssets/The_Sarbanes-Oxley_Act_at_10_-_Enhancing_the_reliability_of_financial_reporting_and_audit_quality/$FILE/JJ0003.pdf Accessed, [2016-04-03]

Finansinspektionen (FI) (n.d.) (2016). Tillstånd av FI eller enbart registrering? Available online: http://www.fi.se/Register/Foretagsregistret/Registrerade-foretag-som-inte-star-under-FIs-tillsyn/ Accessed, [2016-04-03]

Friedman, M. (1970). The Social Responsibility of Business Is to Increase Its Profits. *The New York Times Magazine*, September 13. Available online: http://download.springer.com/static/pdf/525/chp%253A10.1007%252F978-3-540-70818-6_14.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fchapter%2F10.1007%2F978-3-540-70818-6_14&token2=exp=1463039350~acl=%2Fstatic%2Fpdf%2F525%2Fchp%25253A10.1007%25252F978-3-540-70818-6_14.pdf%3ForiginUrl%3Dhttp%253A%252F%252Flink.springer.com%252Fchapter%252F10.1007%252F978-3-540-70818-6_14*~hmac=55792229114de83308db8aafc441712be290ce037e5c3cfe2ad1033102a83149 Accessed, [2016-05-12]

Frink, D. D. & Klimoski R. J. (2004). Advancing accountability theory and practice: Introduction to the human resource management review special edition. *Human Resource Management Review* 14, pp. 1-17. Available online: http://ac.els-cdn.com/S1053482204000026/1-s2.0-S1053482204000026-main.pdf?_tid=6df06568-0d20-11e6-a411-00000aab0f6c&acdnat=1461834541_ea99af646b0e5c142a1ef7416e1974e0 Accessed, [2016-04-27]

Fung, B. (2014). The Demand and Need for Transparency and Disclosure in Corporate Governance. *Universal Journal of Management*. 2(2), p. 72-80. Available online: http://www.hrpub.org/download/20140105/UJM3-12101630.pdf Accessed, [2016-04-04]

Freeman, R. E. (1984). Strategic Management: A Stakeholder Approach (Pittman, Matchfield, MA).

Glaser, B. G. & Strauss, A. L. (1967). The discovery of grounded theory; strategies for qualitative research. Chicago, IL: Aldine Publication.

Harrison, J. S. & Wicks, A. C. (2013). Stakeholder Theory, Value and Firm Performance. *Business Ethics Quarterly*. 23(1), pp. 97-124.

Hill, C.W. & Jones, T.M. (1992). Stakeholder-Agency Theory. *Journal of Management Studies*. 29(2). Available online: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=ff84fa83-46b6-4ee4-989a-e8e33088be11%40sessionmgr120&vid=9&hid=120 Accessed, [2016-04-27]

Isaksson, F, L., Magnusson, K. & Nilsson, M. (2011). Internal control and the COSO model: The five components integration and use within SEB. Linköpings Universitet. Available online: http://www.iei.liu.se/fek/lundh-simon/uppsatser/1.273439/Intern_kontroll.pdf Accessed, [2016-03-25]

Kaplan, R. & Mikes, A. (2015). When One Size Doesn't Fit All: Evolving Directions in the Research and Practice of Enterprise Risk Management. *Journal of Applied Corporate Finance*. Vol. 27(1).

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research 20*, pp. 18–40.

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society 36*, pp. 226– 245.

Mitchell, R. K., Agle, B. R. & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Principle of Who and What Really Counts. *The Academy of Management Review*. Vol. 22(4), pp. 853-886. Available online: http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=5a3fd0a2-37ba-4c26-916f-0c6a6c17ab02%40sessionmgr4005&hid=4205 Accessed, [2016-05-12]

Nasdaq. (2016). Main Market Listings 2014. Available online: http://www.nasdaqomxnordic.com/nyheter/noteringar/main-market/2014 Accessed, [2016-04-01]

Nedaei, B. H. N., Rasid, S. Z. A., Sofian, S., Basiruddin, R. & Kalkhouran, A. B. A. N. (2015). A Contingency-Based Framework for Managing Enterprise Risk. *Global Business and Organizational Excellence*. Vol 34(3), pp. 54-66.

Otley, D. (2016). The contingency theory of management accounting and control: 1980-2014. *Management Accounting Research*. Available online: http://resolver.ebscohost.com/openurl?sid=EBSCO%3aedselp&genre=article&issn=10445005&ISBN=&volume=&issue=&date=20160101&spage=&pages=&title=Management+Accounting+Research&atitle=The+contingency+theory+of+management+accounting+and+control%3a+1980–2014&aulast=Otley%2c+David&id=DOI%3a10.1016%2fj.mar.2016.02.001&site=ftf-live Accessed, [2016-04-27]

Pautz, M.C. & Washington, P. (2009). Sarbanes-Oxley and the Relentless Pursuit of Government Accountability The Perils of 21st-Century Reform. Sage Publications. Vol. 4(6). Available online: http://aas.sagepub.com/content/41/6/651.full.pdf+html Accessed, [2016-03-23]

Potter, J. (1997). ´Discourse Analysis as a way of analysing Naturally Occurring Talk´, in D. Silverman (ed.) *Qualitative Research: Theory, Method and Practice.* London: Sage

Protiviti. (2014). The Updated COSO Internal Control Framework - Frequently Asked Questions. 2nd ed. Available online: http://www.protiviti.se/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf [2016-03-24]

Romney, M. B. & Steinbart, P, J. (2012). Accounting Information Systems. Pearson. 12th Edition.

Romney, M. B. & Steinbart, P, J. (2015). Accounting Information Systems. Pearson. 13th Edition.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2009). Research methods for business students. 5th ed. Harlow, UK: FT Prentice Hall.

SEC. (2008). Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. Available Online: https://www.sec.gov/rules/final/33-8238.htm Accessed, [2016-03-28]

Shin, J. (2012). Resources for Change: The Relationships of Organizational Inducements and Psychological Resilience to Employees'. Attitudes and Behaviours Toward Organizational Change. Available online: http://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?sid=a40417f0-2ad6-4970-b24b-756c76194340%40sessionmgr120&vid=1&hid=120 Accessed, [2016-05-04]

Simons, R. (2013). The Business of Business Schools: Restoring a Focus on Competing to Win. *Capitalism and Society*, Vol. 8(1), art 2. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2084423 Accessed, [2016-05-04]

Simons, R. (2010). Seven Strategy Questions: A Simple Approach for Better Execution. *Harvard Business Press*. Available online: https://books.google.se/books?hl=en&lr=&id=tIYrly9QjTIC&oi=fnd&pg=PR1&dq=Seven+Strategy+Questions:+A+Simple+Approach+for+Better+Execution&ots=iioJV59ihe&sig=IEfCbppVL90DI6BCZt0MpGVya0U&redir_esc=y#v=onepage&q=Seven%20Strategy%20Questions%3A%20A%20Simple%20Approach%20for%20Better%20Execution&f=false Accessed, [2016-05-04]

Stormbal Consulting Home. (2016). A Stakeholder View of Firm, Freeman. Available online: http://stormbal.com/stakeholder-map-freeman-firm/ Accessed, [2016-05-04]

Strebel, P. (1996). Why do employees resist change? *Harvard Business Review,* 74(3), pp. 86-92.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management Review*. 20(3), pp. 571-610.

The Confederation of Swedish Enterprise [Svenskt Näringsliv]. (2007). Corporate Governance, Internal Control and Compliance: From an information security perspective Available online: http://www.svensktnaringsliv.se/migration_catalog/Rapporter_och_opinionsmaterial/Rapporters/corporate_governance_10017apdf_579086.html/BINARY/Corporate_Governance_10017a.pdf Accessed, [2016-03-24]

The Institute of Internal Auditors. (2008). Sarbanes-Oxley section 404: a guide for management by internal controls practitioners. *The institute of internal auditors*. 2nd Edition, January 2008. Available online: https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf Accessed, [2016-03-24]

The Swedish Corporate Governance Board [Kollegiet för svensk Bolagsstyrning]. (2015). Svensk kod för bolagsstyrning. *Kollegiet för svensk Bolagsstyrning*. Available online: http://www.bolagsstyrning.se/media/69007/svenskkodbolagsstyrn_2015_151124.pdf Accessed, [2016-03-24].

The Swedish Parliament [Sveriges Riksdag]. (2016). Årsredovisningslag (1995:1554). Available online: https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/rsredovisningslag-19951554_sfs-1995-1554/ Accessed, [2016-04-04]

Tufano, P. (1996). Who manages risk? An empirical examination of risk management practices in the gold mining industry. *Journal of Finance 51*, pp. 1097–1137.

Wendt, J. (2016). Interviewed by Ewerbring and Klingvall. Malmö, 30 March 2016.

Yin, R.K. (2009). Case study research: design and methods. Thousand Oaks: Sage Publications, 4th ed.

Yin. (2012). Applications of Case Study Research. Sage Publications Inc. 3rd Edition. Available online: https://books.google.se/books?hl=sv&lr=&id=FgSV0Y2FleYC&oi=fnd&pg=PR1&dq=A+(VERY)+BRIEF+REFRESHER+ON+THE+CASE+STUDY+METHOD&ots=41c8TtqnRp&sig=fckLiGR6262I_O8ghMufN7XNgD0&redir_esc=y#v=snippet&q=The%20case%20study%20method%20embraces%20the%20full%20set%20of%20procedures%20needed%20to%20do%20case%20study%20research.%20These%20tasks%20include%20designing%20a%20case%20study%2C%20collecting%20the%20study%E2%80%99s%20data%2C%20analyzing%20the%20data%2C%20and%20presenting%20and%20reporting%20the%20results.%20(None%20of%20the%20tasks%2C%20nor%20the%20rest%20of%20this%20book%2C%20deals%20with%20the%20development%20of%20teaching%20case%20studies%E2%80%94frequently%20also%20referred%20to%20as%20the%20%E2%80%9Ccase%20study%20method%E2%80%9D%E2%80%94the%20pedagogical%20goals%20of%20which%20may%20differ%20entirely%20from%20doing%20research%20studies.)&f=false Accessed, [2016-04-03]

# Appendix

## Appendix 1: Interview Guide - Jonas Wendt

**Interview Guide Jonas Wendt**

***Authors:***

*Ewerbring, Josephine:*
*Phone number 0703226090*
*Klingvall, Fredrik*
*Phone number: 0768035282*

**Questions**

1. Should we focus on how Enterprise Risk Management is implemented? Or do you think it is also good to investigate why they chose to implement ERM?

2. Would it be interesting to research if problems and difficulties are different between the companies?

3. Do you think we should investigate the two different companies' COSO frameworks and compare them? Or should we compare companies with COSO and COSO ERM? Since comparability is important?

4. Do you have any suggestions for which companies we should choose? Industry and company? Reason?

5. Do you have any suggestions of how we should get in contact with the specific companies?

## Appendix 2: Interview Guide English - CFO

**CFO Interview Guide**

***Authors:***

*Ewerbring, Josephine:*

*Phone number 0703226090*

*Klingvall, Fredrik*

*Phone number: 0768035282*

**General Question - Section (i)**

1. In general how would you describe the risk management practises of the company on a holistic level?

---

**Internal Control Principles - Section (ii)**

1. **Control environment**: What is your view on the company's internal control environment, i.e. Culture, structure and responsibilities?
2. **Risk assessment**: Do you work with risk assessment and risk handling in your organisation?
3. **Control activities**: Does the company have any control activities for mitigating the risks that you described?
4. **Information and communication**: How does the information of risks flow within the company? How does the communication work?
5. **Monitoring**: Do you have on-going revision of the risks and controls that the company is affected by?

---

**Enterprise Risk Management - Section (iii)**

1. Do you work with risk on a strategic level?
2. How do you view risk in terms of the company's risk appetite? Do you work within a specific risk appetite or do you try to mitigate all risks?

---

**Ending Questions - Section (iv)**

1. Is anything difficult or problematic regarding risks and controls within the company?
2. How successful are each of the COSO dimensions implemented on a scale of 1-5 in the company according to you?

## Appendix 3: Interview Guide Swedish - CFO

**CFO Intervjuguide**

***Författare:***

*Ewerbring, Josephine:*
*Telefonnummer: 0703226090*
*Klingvall, Fredrik*
*Telefonnummer: 0768035282*

**Generella frågor - Avsnitt (i)**

1. Hur skulle du generellt beskriva företagets riskhantering på en övergripande nivå?

---

**Interna kontrollprinciper - Avsnitt (ii)**

1. **"Control environment"**: Hur ser du på företagets interna kontroll-miljö. Dvs. Kultur, struktur och ansvarsfördelning?
2. **"Risk assessment"**: Arbetar ni med att hantera risker i er organisation?
3. **"Control activities"**: Har företaget några kontroller för att begränsa riskerna du beskriver?
4. **"Information and communication"**: Hur flödar information om risker i organisationen? Hur går kommunikationen till?
5. **"Monitoring"**: Har ni en ständigt pågående revision av risker och kontroller som bolaget påverkas av?

---

**Enterprise Risk Management - Avsnitt (iii)**

1. Arbetar ni med risk på strategisk nivå?
2. Hur ser ni på risk i förhållande till er riskaptit? dvs. Arbetar ni inom en riskaptit eller försöker ni förhindra alla risker?

---

**Avslutande frågor - Avsnitt (iv)**

1. Anser du att något är svårt eller problematiskt angående bolagets riskhantering?
2. Hur framgångsrikt är varje del av COSO:s dimensioner implementerade på en skala 1-5 inom bolaget enligt dig?

## Appendix 4: Interview Guide English - Financial Assistant

**Controller Interview Guide**

***Authors:***

*Ewerbring, Josephine:*
*Phone number 0703226090*
*Klingvall, Fredrik*
*Phone number: 0768035282*

**General Question - Section (i)**

1. Does the company use any risk frameworks, or structured processes for control?

---

**Internal Control Principles - Section (ii)**

1. **Control environment**: What is your view on the company's internal control environment, i.e. Culture, structure and responsibilities?
2. **Risk assessment**: Do you work with risk assessment and risk handling in your organisation and division?
3. **Control activities**: Does the company have any control activities for mitigating the risks that you described?
4. **Information and communication**: How does the information of risks flow within the company? How does the communication work?
5. **Monitoring**: Do you have on-going revision of the risks and controls that the company is affected by?

---

**Enterprise Risk Management - Section (iii)**

1. Do you work with risk on a strategic level?
2. How do you view risk in terms of the company's risk appetite? Do you work within a specific risk appetite or do you try to mitigate all risks?

---

**Ending Questions - Section (iv)**

1. Is anything difficult or problematic regarding risks and controls within the company?
2. How successful are each of the COSO dimensions implemented on a scale of 1-5 in the company according to you?

## Appendix 5: Interview Guide Swedish - Financial Assistant

**Controller Intervjuguide**

***Författare:***

*Ewerbring, Josephine:*
*Telefonnummer: 0703226090*
*Klingvall, Fredrik*
*Telefonnummer: 0768035282*

**Generella frågor - Avsnitt (i)**

1. Hur skulle du generellt beskriva företagets riskhantering på en övergripande nivå?

---

**Interna kontrollprinciper - Avsnitt (ii)**

1. **"Control environment"**: Hur ser du på företagets interna kontroll-miljö. Dvs. Kultur, struktur och ansvarsfördelning?
2. **"Risk assessment"**: Arbetar ni med att hantera risker i er organisation och din division?
3. **"Control activities"**: Har företaget några kontroller för att begränsa riskerna du beskriver?
4. **"Information and communication"**: Hur flödar information om risker i organisationen? Hur går kommunikationen till?
5. **"Monitoring"**: Har ni en ständigt pågående revision av risker och kontroller som bolaget påverkas av?

---

**Enterprise Risk Management - Avsnitt (iii)**

1. Arbetar ni med risk på strategisk nivå?
2. Hur ser ni på risk i förhållande till er riskaptit? dvs. Arbetar ni inom en riskaptit eller försöker ni förhindra alla risker?

---

**Avslutande frågor - Avsnitt (iv)**

1. Anser du att något är svårt eller problematiskt angående bolagets riskhantering?
2. Hur framgångsrikt är varje del av COSO:s dimensioner implementerade på en skala 1-5 inom bolaget enligt dig?

## Appendix 6: COSO Internal Control Framework's 17 Principles

**Control Environment**

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

**Risk Assessment**

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

**Control Activities**

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

**Information and Communication**

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

**Monitoring activities**

16. The organization selects, develops, and performs on-going and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.