Master Thesis:

Risk Management

Differences in Use Between Public and Private Organizations

Benchmarking Municipalities from an Enterprise Perspective

Authors:

Sofie Dersén

Hanna Warnander

Supervisor:

Anna H Glenngård

Abstract

Seminar date: 30 May 2016

Course: BUSN 68 Degree Project - Accounting and Management Control 15 credits

Authors: Sofie Dersén, Hanna Warnander

Advisor: Anna H. Glenngård

Five key words: Risk management, management control, COSO, public organizations, private organization

Purpose: The purpose of the study is to contribute to the knowledge on the use of risk management and especially ERM in different context. More specifically the aim is to find what similarities and differences there are in the use of ERM between public and private sector, as well as to find what variations there are within each sector.

Methodology: The method used during this multiple case study, is an inductive approach with a qualitative strategy. Documents from two private organizations and two public organizations have been reviewed, as well as semi-structured interviews conducted with employees in each organization.

Theoretical perspectives: For the theoretical perspective framework, the legitimacy theory, stakeholder theory, levers of control and management control systems package has been used. The practical framework mainly consists of internal control and its framework as well as enterprise risk management and its framework.

Empirical foundation: The empirical foundation consists of documents and interviews. The results have then been presented in accordance to sector and has further been divided into themes for an accessible overview.

Conclusions: An indication was found that despite different conditions and stakeholders, all respondents work with risk management. Further indication show that the definition of ERM is most likely not crucial. Even though the municipalities have several documents clarifying the responsibility of internal control but the responsibility might not be as clear in reality.

Acknowledgments

Table of contents

1. Introduction

This chapter starts with introducing Enterprise Risk Management and presenting previous research on the topic within the private as well as the public sector. Thereafter a problematization is formalized which then narrows down to the purpose. Limitations and finally a short description of the thesis will follow.

1.1 Background

In order to get a deep understanding of an organization and how to control it, managements and boards try to predict the future and map their surroundings. Both public and private sector organizations have their internal control regulated in the Swedish law. The organizations need to adjust their internal control to The Swedish Local Government Act respectively The Swedish Companies Act (Munck, 2014). Furthermore, World Economic Forum (2016, p. 8) states that "*Risks are becoming more imminent and have wide-ranging impact*". Meaning that the demand for enterprise risk management (ERM) is not only increasing in the private sector, but continually growing in the public sector (PWC, 2015). The public sector have been influenced by private sector management styles the last decades, which New Public Management (NPM) is an example of (Lapsley, 2009). As a result, the public sector needs to apply private sector management tools and their accounting norms (Hood, 1995). This includes tools for internal control.

The leading organization within internal control and ERM is COSO. COSO stands for Committee of Sponsoring Organizations of the Tradeway Commission (McNally, 2013). It is a private-voluntary organization with an aim of improving the performance and governance of organizations' via internal control, ERM and fraud deterrence. They have been publishing frameworks regarding these subjects since 1992 (McNally). COSO was originally founded in 1985 as a sponsor to the National Commission on Fraudulent Financial Reporting (COSO, 2004). Their objective was to study the factors that could lead to fraudulent behaviour and to come with recommendations to public companies and their auditors.

1.2 Previous Research

1.2.1 The Rise of ERM

Bromiley et al. (2015) state that when it regards risk, finance and accounting research has highlighted *"tools that apply only to risk with well-defined statistical properties."* (p. 625). Further, it is claimed that the discussions in risk management has not been prioritized. They mention that the academic research seldom is published in management journals, thus they interpret it as if the ERM is still being developed.

According to Dickinson (2001), risk management has been part of decision-making since 1940's. Though the corporate concept of ERM did not appear until the mid-1990's. Dickinson states that ERM has two purposes, where the first is to widen the scope of corporate governance, as a reaction to scandals and failures that could have been prevented. The second reason for existing, is due to increasing importance of shareholder value models concerning strategic planning. Furthermore, Dickinson mention that the more comprehensive approach of risk management appeared from a wider management thinking. This is supported by Bromiley et al. (2015), who suggest that ERM includes all the risks of an organization and deal with them extensively instead of one by one. They continue by stating that organizations previously have handled risks separately. Which was due to different divisions in the organization focusing on different parts of risk.

Dickinson (2001) continues by defining enterprise risk as *"the extent to which the outcomes from the corporate strategy of a company may differ from those specified in its corporate objectives, or the extent to which they fail to meet these objectives"* (2001, p. 361). He states that internal and external factors can affect a company's outcomes and differentiate from its intended goals. Some of these factors can thus be interpreted as risks.

1.2.2 ERM in the Public Sector

Knutsson et al. (2008) state that the public sector is a large sector in Sweden and most of the activities occur in the municipalities. The municipalities deal a lot with regulated activities and also activities that add to the public interest. Furthermore, it is stated that the competence

and efficiency of adapting to new management methods is of importance for the public sector. Lapsley (2009) as well as Courpasson and Reed (2004) mention that public sector organizations get a lot of influence from the private sector. Risk management is one of the latest trends to arrive within the public sector in the U.K., according to Lapsley. Although, risk management is also being mentioned as an abuse. Further, Lapsley considers risk management to be a strategy only implemented to improve the reputation of the public sector. Palermo (2014) claims that risk management in the public sector can lead to lowering insurance premiums and cost of borrowing. This could be considered as a way of improving reputation, as previously mentioned. Lapsley continues by stating that risk management can appear neutral and impartial to the public managers in their strive for balance between risk avoidance and being entrepreneurial.

1.3 Problematization

Bromiley et al. (2015) summarize definitions of ERM from academic journals as well as from standard setting organizations, rating agencies etc. as a means to highlight the need for a single definition of the ERM concept. Lapsley (2009) argues that public sector is a large part of society and that more tools from the private sector is being implemented. However, the research on the use of the tools of risk management is still limited, according to Bromiley et al. (2015). Thus, making it interesting to investigate the variations in how risk management is used within the different sectors.

1.4 Purpose

The purpose of the study is to contribute to the knowledge on the use of risk management and especially ERM in different contexts. More specifically the aim is to find:

1. What similarities and differences are there in the use of ERM between public and private sector?
2. What variations are there in the use of ERM within the public sector respective within the private sector?

1.5 Limitations

The focus of the study will be on risk management and ERM, while some consideration will be taken to the use of internal control in the organizations. The narrow selection of only choosing two private organizations and two public organizations will give the thesis an indication that can be developed in future research.

2. Methodology

The methodology being used in this thesis is an inductive method with a qualitative direction. The study has been performed with the help of a multiple case study, which means that the foundation consists of interviews and documents from the chosen organizations. Finally, the ethical problems of the study will be mentioned.

2.1 Research Approach

Bryman and Bell (2015) mention that through a development process when collecting data, inductive theories and concepts are gathered. This mean that the new findings is complementing the base of theories that already exists. Bryman and Bell furthermore state that the inductive method is often, but not always, used in combination with a qualitative research strategy. Additionally, it is mentioned that there exists three different types of methods within the inductive strategy. Theory-testing research, inductive case research and interpretive research (Bryman & Bell, 2015). The theory-testing research is based on developing hypothesis from previous research. The hypothesis is later confirmed or unconfirmed. Inductive case research is based on developing theory using qualitative data. The point of this method is to be able to test theories. Finally, the interpretive research bases its research on qualitative data too, though the theory is not developed in the same way as the inductive case research strategy. Instead, a dialogical process is performed between theory and empirical phenomenon. Which means that the result will not be explanatory or come with theoretical suggestions. The approach chosen for this thesis is the interpretive research method. Reviewing documents and conducting interviews have laid the foundation for the dialogical process.

An alternative to the inductive method is the deductive method, which means that the result of the study is based on hypothesis, according Bryman and Bell (2015). The reason for not choosing the deductive method is due to the perception that the inductive method, and more specifically the interpretive research, would fit the purpose of the thesis better.

2.2 Research Strategy

According to Bryman and Bell (2015), a study can have two directions. Either the quantitative or the qualitative direction. A qualitative study, is not focusing on statistical connections but rather on substance (Alvehus, 2013). This kind of study can be conducted by interviews, observations or focus groups (Bryman & Bell, 2015).

The other direction mentioned, a quantitative study means that the authors conduct surveys, structured interviews or observations (Bryman & Bell, 2015). Thus, having a large selection of respondents to help answering the research question. This also means that the answer will be wider and more generalizable. The aim of this thesis is to go in deep and narrow into the research question, which is why the qualitative research strategy has been chosen.

Though, Bryman and Bell (2015) present some criticism of qualitative research. They argue that it can be viewed as too subjective, difficult to replicate, problems of generalization and lack of transparency. The issue of replication is reduced by publishing the interview guides. The problem of generalization is excluded, since the results only should be seen as an indicator and not to be representative for the entire population. Additionally, the lack of transparency is decreased by presenting an extensive explanation of how the sampling was made and why.

2.3 Multiple Case Study

A multiple case study method can be used when there is a need for understanding complex social events (Yin & Nilsson, 2007). This method is commonly applied when questions regarding "how" or "why" needs to be answered. The purpose of the method is to contribute with knowledge about organizational, individual and social factors among others.

A normal question regarding case studies is if it is possible to make generalizations based on one case, according to Yin and Nilsson (2007). Furthermore, Yin and Nilsson claim it is possible to compare case studies to experiments, due to the same course of action in the two methods. Thus, making it possible to make generalizations based on a case study. It is

moreover mentioned that multiple case studies can be performed during a shorter time period, though the method has been criticized for not showing exact results. Also, it is stated that the most common way of collecting information for a case study is by conducting interviews.

The case study is performed on two municipalities and two companies and only conducted under a short period of time. The documents that are being reviewed is the latest version of their financial statement. Furthermore, documents, also most recent version, containing internal control or risk management as well as the websites have been inspected. The reason for only examining the most recent version of the documents, is that focus has not been put on the change within the organizations from year to year, but rather on similarities and differences between the organizations.

2.3.1 Sample

There are two types of sampling presented by Bryman and Bell (2015); probability sampling and purposive sampling. Probability sampling defines a sample selected by a random selection method, where each unit in a population has a chance of being selected. In contrast, purposive sampling is a non-probability type of sampling, where the sampling is collected in a strategic way. Bryman and Bell describe two criteria that can be used when choosing the method of sampling. Firstly, if it is important to generalize the results to a wider population, probability sampling is preferred according to Bryman and Bell. In order to generalize the result, the sample have to be representative of the total population (Bryman & Bell, 2013). Secondly, if the research questions gives an indication that a certain category should be sampled, the purposive sampling is most likely used (Bryman & Bell, 2015).

However, the purpose of this thesis is not to make a general contribution of how ERM is used throughout the public and private sector, but instead to give indicators of how it ought to be. Furthermore, the research questions gives an indication of that both the actors in the public and private sector, working with ERM, should be investigated. As a result, purposive sampling was used. More specifically, generic purposive sampling was used, which implied that the researcher defined criteria that needed to be fulfilled, in order to answer the research questions. Following of, identifying appropriate cases and selecting a sample based on those

criteria (Bryman & Bell, 2015). The size of the sample was dependent on the required amount of comparisons between groups within the sample. Because of the chosen strategy, two municipalities and two companies have been selected, which enabled cross comparison as well as in depth study of their documents.

Recently a study by Håkansson, Jakobsson and Lundin (2015) was published. These authors investigated all municipalities in Scania and developed a table. They specified how well developed the municipalities work with risk management was. The selection of this thesis is based upon the results from Håkansson, Jakobsson and Lundin (2015). The municipalities working with risk management and not solely internal control, was further reviewed through their annual reports, websites and other documents. Municipality 1 and 2 were perceived to publish the most information about risk management and were therefore chosen and contacted.

The study was delimited to only consider large organizations, since they are most likely to have a high focus on ERM. Regarding their location, it was narrowed to Scania, due to convenience. The selection of private organization started with visiting the website allabolag.se, to view companies located in Scania and showing them according to their turnover. Thereafter, the annual reports and websites was searched to see who used COSO and risk management in the reports. Finally, the Companies 1 and 2 were selected and contacted.

2.3.2 Interviews

Bryman and Bell (2015) state that the main types of interview in qualitative studies are unstructured interviews and semi-structured interviews. During an unstructured interview, the researcher solely relies on some notes, to help cover a certain set of topics. In comparison, the researcher prepare a fairly specific list of questions and topics to cover, referred to as interview guide, before a semi-structured interview.

Bryman and Bell (2015) argue that a semi-structured interview should be used when the researcher has a fairly clear focus on what to investigate in the beginning of the research.

Moreover, this method is also to prefer during a multiple case study research, since it enables cross-case comparability and was therefore used. However, the interview guide was somewhat individualized to each organization, based on their published documents. According to Yin (2014) it is of importance to be adaptive when conducting interviews. He furthermore states that interviews seldom end up exactly the way they were planned. The respondents were given the questions in advance, allowing them to prepare their answers as well as contact other employees for more information. Moreover, this might have increased the comfortability of the respondents.

2.3.3 Respondents

The respondents from the organizations were chosen by the organizations themselves. After initial contact was taken, a recommendation was given on the most appropriate person or persons to interview. This recommendation was based on a description on the subject of the thesis. Although, in Municipality 1, there was some confusion regarding who should answer the interview questions. This lead to several persons recommending someone else as a respondent for the study.

The respondent from Company 1 is working as the manager of Accounting and Taxes. In Company 2, the respondent is working as the manager for internal control and is a member of the company's ERM board. In Municipality 1, one respondent is working as a security strategist and the other respondent work as an administrator. The final respondent, from Municipality 2, is a CFO. The difference of work chores among the respondents can of course be reflected in the answers given. Though, since all of the respondents are considered experts in the areas, by their employees, the selection should be considered valid.

Two of the interviews were performed on location, one on the phone and the final one via Skype without camera. This means that different impressions were given both by the respondents as well as the researchers. All of the interviews were performed by both researchers in order to support and ask follow up questions when needed. The duration of the interviews varied, the shortest took 24 minutes and the longest took an hour.

Respondents	Title	Date	Time spent on interview	How interview was performed
Company 1	Manager of Accounting and Taxes	19 April 2016	39 minutes	Skype
Company 2	Manager of internal control and member of ERM board	2 May 2016	24 minutes	Phone
Municipality 1	Security strategist and administrator	22 April 2016	60 minutes	On location
Municipality 2	CFO	28 April 2016	32 minutes	On location

Table 1: Conduction of interviews

2.3.4 Interview Guide

Bryman and Bell (2015) state that an interview guide is less advanced than a structured interview schedule. They claim that it can be compared to a short list of areas to cover during the interview. This is presented as an accepted way of conducting semi-structured interviews. Moreover, the point of an interview guide is to let the respondents know in what direction the interview is heading.

It is advised by Bryman and Bell (2015) to start the interview with introducing questions. Therefore each interview began with questions regarding the respondent's background and their current tasks. Thereafter the questions in the interview guide were asked. However, following up questions as well as interpreting questions were asked between the prepared questions. This in order to develop the answers or continue on an interesting subject.

The empirical result as well as the analysis and discussion have been based on themes when presented. The themes that have been chosen are: Definition of ERM, Framework, Who

works with ERM, The work of ERM, Impacts. All the themes are based on the questions asked during the interviews (Appendix). These areas were chosen in order to give an overview of the work within risk management.

2.3.5 Documents

The document that have been reviewed and analyzed have been found on the companies and municipalities websites. In some cases, more documents have been received from the respondents in order to complement the information already found. In all the cases, the financial statement have been analyzed and this information have been the foundation of the selection of municipalities and companies. Additional documents containing information about risk management have been included, since not all respondents publishes the main part of the risk management in their financial statements.

2.4 Method Criticism

2.4.1 Reliability

Reliability includes how well the members of the research team agree of what they observe (Bryman & Bell, 2015). The reliability has been increased by recording all interviews and transcribing each interview. Thus, allowing the researchers to go through the material several times, in order to receive and present a fair view of what was said. Additionally, the documents was first investigated alone by each researcher and then discussed. This has permitted the researchers to receive an opinion of their own, before discussing and analyzing.

2.4.2. Replicability

The replicability of a study is the degree to which the study can be replicated (Bryman & Bell, 2015). They argue that it is difficult to achieve in a qualitative study, since it is impossible to freeze a social setting. Nonetheless, by publishing the interview guide (Appendix) it improves the ability to replicate the study. Although, since semi-structured interviews have been used it was only the basic questions that have been presented and not the ones that were asked spontaneous during the interviews. Further, an extensive description

of the sample made was presented. However, since all the organizations were anonymous, it makes it impossible to use the same respondents in another study performed by different researchers. The researchers were allowed to name the municipalities, which was disregarded in order to remain consistent throughout the study.

2.4.3 Validity

Internal validity describe how good matching there is between researchers' observations and the theoretical ideas they develop (Bryman & Bell, 2015). In comparison, external validity concern whether the study's results can be generalized or not. Nevertheless, since purposive sampling has been used, it has been impossible to generalize the results to the entire population. Instead, the study has given an indication of how ERM is being used in different contexts.

Another limitation of the study is inconsistency concerning the interviews. The best way would be if all interviews had been conducted the same way. But since leaving the decision up to the respondent, whether the interview should be conducted via phone, Skype or in person, it was not up to the researchers. The reason for letting the respondents decide how the interview should be conducted was to make the respondents feel comfortable and that the researchers were showing compliance. Further, letting the organizations themselves decide whom to interview, could be discussed whether or not it was a wise decision. Having flexibility when wanting someone else to spend time on you when conducting interviews could be of advantage. Though, it lead to interviewing respondents within different work areas, which could have had an effect on the result.

3. Theoretical Perspectives

This chapter introduces the theories that will be applied to the result later on in the thesis. Legitimacy theory, stakeholder theory, levers of control and management control systems package are all being mentioned.

3.1 Legitimacy Theory

Throughout this thesis the definition of legitimacy will be "*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 definition*s." (Suchman, 1995, p. 574). According to Deegan and Unerman (2011) the legitimacy theory claims that organizations try to secure that they are perceived as operating in accordance with the limits and norms of their societies on a regular basis. These limits and norms of the society forms a social contract with the organization, which becomes the foundation of the theory. Moreover, it is stated that these social contracts consists of several terms and conditions that are more or less explicit.

Deegan and Unerman (2011) furthermore mention that as a way of gaining and maintaining legitimacy, different strategies will be performed by the organization. These strategies may include taking steps like controlling or working in collaboration with other parties, that are perceived as legitimate (with the intention that the legitimacy of the party will be transferred to the organization in question) alternatively, by using target disclosures.

When the social contract is not perceived as fulfilled, the term legitimacy gap is being used by Deegan and Unerman (2011). Sethi (1978) mentions that a legitimacy gap can be created by the difference between how the organization perform and the expectations that society have on the organization. Though, it is important to have in mind that these expectations change over time. If the organization does not adapt after the expectations, legitimacy and the life of the organization can be lost. Sethi (1977, mentioned in Deegan & Unerman, 2011) also mentions another way to create a legitimacy gap, that is by releasing information about an organization that previously was not known to the public.

3.2 Stakeholder Theory

Freeman and Reed (1983, p. 91) defines a stakeholder as *"Any identifiable group or individual who can affect the achievement of an organisation's objectives, or is affected by the achievement of an organisation's objectives"*. This definition will be used through the thesis.

Deegan and Unerman (2011) claim that the aim of the stakeholder theory is to show how an organization interacts with their stakeholders. It is divided in two categories, ethical and positive branch, where the ethical branch refers to the moral and normative perspectives and the positive branch refers to the managerial perspective. The ethical branch argues for the right of the stakeholders to be treated reasonably by the organization. The positive branch on the other hand is about the problems regarding stakeholder power and how that power affects the ability to force the organization to act in accordance to expectations of the stakeholders (Deegan & Unerman, 2011).

Clarkson (1995) divide up the stakeholders even more. He mentions primary stakeholders as the stakeholder whose participation the organization needs for its survival. The secondary stakeholder is the participator that is involved in the organization but is not crucial for survival. Thus, according to this perception the primary stakeholder is the one that management has to take the most consideration to.

Deegan and Unerman (2011) continue with explaining that in the descriptive positive branch of the stakeholder theory, the organization is part of a more extensive social system. They furthermore state that this branch takes consideration to many different stakeholder groups within the society. This could be interpreted as something that municipalities need to do continually since the society is considered to be the largest stakeholder. Moreover, Deegan and Unerman mention that these stakeholder groups will try to impact the decisions made in the organization. They continue by stating that it is impossible for the organization to respond to all its stakeholders, thus have to limit the responses to those assumed to be the most influential. Furthermore, it is mentioned that public sector is more likely to act in accordance

to the environmentalists (Neu, Warsame & Pedwell, 1998). The private sector on the other hand, is found more likely to act in accordance to the financial stakeholders.
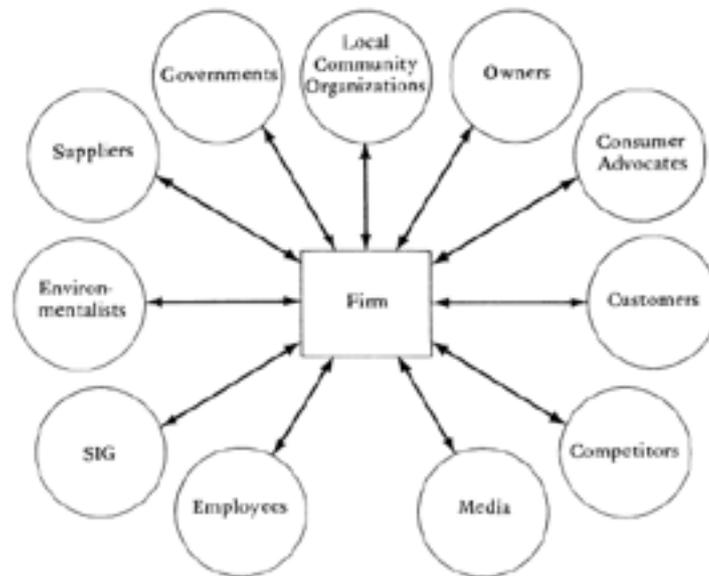
Figure 1: Stakeholder map (Freeman, 1984)

According to Knutsson et al. (2006), the stakeholders of a municipality can be identified as the government, citizens, politicians and constituents, producers, customers, employers and employees, companies, trade associations, media and collective activities among others. They furthermore state that when the amount of stakeholders increase, the strength and number of wills to take consideration to increase in turn. It is claimed that this can affect the municipality and cause insecurity and unclear directions in achieving organization's targets. Moreover, Knutsson et al. mention that diverse stakeholder groups affect the parts of a municipality in different ways, thus leading towards a variety of prioritization within the organization.

Figure 2: Examples of a municipality's stakeholders (own model)

3.3 Levers of Control

Simon's (2000) framework of four levers of control consist of; diagnostic control systems, interactive control systems, belief systems and boundary systems. Diagnostic control systems are defined as the formal information systems managers use when measuring and monitoring the organizational outcomes. After comparing the actual outcome to the budgets and performance goals, corrective actions is taken based on the deviations. This enable the managers to improve the inputs and processes and lessen deviations in the future. According to Simon, diagnostic control systems is used to implement the strategy efficiently and to preserve scarce management attention. In comparison, the interactive control systems focuses on the strategic uncertainties of the organization (Simon). This formal information system, helps managers to be more involved in the subordinates' decisions as well as making them focus on the major strategic issues (Romney & Steinbart, 2015).

In order for organizations to ensure that the employees engage in the expected activities, managers must develop a strong set of core values (Simon, 2000). He claims that the communication of core values can be handled informally within small organizations, compared to larger organizations where this is accomplished by formal belief systems. Belief systems define how the organization creates value, encourage the employees to understand

the management's vision, communicates the core value of the company and influence the employees to follow (Romney & Steinbart, 2015). In addition, boundary systems needs to be established in order to communicate what risks to avoid, based on the business strategy (Simon, 2000). Furthermore, boundary systems encourage employees to act ethically, creatively solving problems and meeting customer needs. However, they should still meet minimum levels of performance, avoid off-limit activities and be careful to not damage the company's reputation (Romney & Steinbart, 2015).

3.4 Management Control Systems Package

Malmi and Brown (2008, p. 290-291) define management control as "*management controls include all the devices and systems managers use to ensure that the behaviours and decisions of their employees are consistent with the organisation's objectives and strategies, but exclude pure decision-support systems. Any system, such as budgeting or a strategy scorecard can be categorised as a MCS*", which is consistent with the view of Management Control Systems (MCS) in this thesis.

The framework of MSC consists of five types of controls; planning, cybernetic, reward & compensation, administrative and cultural controls (Malmi & Brown, 2008). The planning controls can be both short-term and long-term. The action planning is where actions and goals are established for the nearest future, usually within one year and it has tactical focus. Whereas, the more strategic focus lies within the long-range planning, where actions and goals are established for a longer period. Cybernetic controls, is where performance is quantified, measured and compared to standards. The information is then analyzed and the system modified. The components of cybernetic controls is budgets, financial measures, non-financial measures and hybrids, which contains both financial and non-financial measures. The third element, reward & compensation controls, focuses on motivating and increasing the performance of the organizational members (Bonner & Sprinkle, 2002). Bonner and Sprinkle present how the effort of the employees increase by attaching incentives and rewards to controls.

Administrative control systems is where the employee's behaviour is directed by organizing individuals and groups, monitoring, specifying codes of conduct and lastly to whom the employee should be held accountable for its behaviour (Malmi & Brown, 2008). They include three groups of administrative controls; organization design & structure, governance structure within the firm and the procedures & policies. Organizational design can help to establish certain kind of contact and relationship. Additionally, organizational structure helps controlling by reducing the inconsistency of behaviour and thereby make it easier to predict (Flamholtz, 1983). Governance is the formal guidelines of authority and accountability. The governance includes the structure and composition of the board and other management teams (Abernethy & Chua, 1996). The final element, cultural controls, consist of; symbol-based controls, value-based controls and clan controls (Malmi & Brown, 2008). Value-based controls is similar to Simon's (2000) belief systems. Symbol-based controls relates to the visual expressions an organization creates, for instance dress codes and buildings, in order to develop a certain culture (Shein, 1997). It was Ouchi (1979) who developed the concept of clan control, which means that organization controls is reached by developing values and beliefs through rituals and ceremonies.

3.5 Chapter Summary

Within the legitimacy theory it is claimed that organizations' strive after achieving status and confirmation from society (Deegan & Unerman, 2011). A mean of achieving this status is by operating according to social contracts, which states limits and norms the organization must follow. Deegan and Unerman continue by claiming that organizations also seek approval from its stakeholders. Though, the private and public sector stakeholders differ from each other, some stakeholders are shared. An example of a shared stakeholder can be the government, but also the society, employees or anyone who has an interest in the organization and its success.

Simon (2000) on the other hand presents four controlling systems. The first to control measures and monitor outcomes. The next control system involves managers in employees' decision-making. The third is emphasizing communication within the organization and the last control is about acting in accordance with company's guidelines. Malmi and Brown's

(2008) control package follow up on the topic with five controls; planning, cybernetic, reward & compensation, administrative and cultural control. These controls can be seen as directions for employees, on how to live up to employers' demands of what and how an employee should be acting like, and how the organization should be seen by others.

4. Practical framework

The practical framework introduces the internal control, its framework as well as enterprise risk management and its framework. These frameworks are both created by COSO and they are the foundation of the thesis. Some differences between them and some critique towards ERM will also be presented. The chapter will end with ERM in public organizations.

4.1 Internal Control

COSO (2013, p. 3) define internal control as "*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*". Internal control can be of three different types; preventive controls, detective controls and corrective controls (Romney & Steinbart, 2015). Preventive controls discovers problems before they occur. Contradictory, detective controls identifies problems that have not yet been prevented. Finally, corrective controls both discover and correct problems and recover from the subsequent errors (Romney & Steinbart).

4.1.1 The Internal Control - Integrated Framework

COSO released a framework for internal control (IC) in 1992, which was updated in 2013 due to changing environment. Globalization, the pace and complexity in rules as well as changing business models all contributed to the update in the framework, according to McNally (2013). It is also stated that nowadays there are higher expectations on risk management as well as detecting and preventing fraud from the perspective of stakeholders.

The IC Framework consists of five components that are of great importance for the framework: control environment, risk assessment, control activities, information & communication and finally monitoring activities (McNally, 2013). The purpose of these components are to relieve the identification, monitoring and balance of the risks.

Additionally, the Framework have 17 principles according to Romney and Steinbart (2015). They also mention that the IC Framework contributes with more specific and exact directions

on how to apply the Framework and the documentation of it. In the control environment of the IC Framework, there are five underlying principles, the risk assessment contains of four principles, control activities and information & communication each have three principles and the monitoring activities have the final two principles (McNally, 2013).

Figure 3: Internal Control - Integrated Framework (COSO, 2013)

4.2 Enterprise Risk Management

Frigo and Anderson (2011, p. 5) define ERM, just like COSO, as "*a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*"

Romney and Steinbart (2015) mention some principles that is the foundation of ERM. These principles states that (p. 221):

- *"Companies are formed to create value for their owners.*
- *Management must decide how much uncertainty it will accept as it creates value.*
- *Uncertainty results in risk, which is the possibility that something negatively affects the company's ability to create or preserve value.*
- *Uncertainty results in opportunity, which is the possibility that something positively affects the company's ability to create or preserve value.*
- *The ERM Framework can manage uncertainty as well as create and preserve value."*

26

4.2.1 Enterprise Risk Management - Integrated Framework

Some years after the release of the IC Framework in 1992, COSO found that there did not exist a common foundation for managements and boards to evaluate risk management (COSO, 2004). This lead to developing the ERM Framework, with an aim to create a benchmarking method for the organizations. This Framework focuses on how to identify risks, threats and opportunities to improve stakeholder value. Faris et al. (2013) state that the ERM Framework can contribute with operational and strategic advantages in the complex world that organizations operate in today.

The ERM Framework model consists of three dimensions according to Romney and Steinbart (2015). The first dimension is the risk and control elements, the second represents the four objectives and lastly the company and its subunits. The dimension of risk and control elements contain the dimension of internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication and finally, monitoring.

The internal environment is about the company's culture, how is assesses and responds to risk, according to Romney and Steinbart (2015). The second component, the objective setting, is about visions, what is hoped to be achieved. Thirdly, the event identification includes both events with positive and negative impacts and it represents uncertainty. Risk assessment & risk response is the fourth component, which is based on the objective setting. It is stated that risks can be acknowledged in four ways; reducing, accepting, sharing or avoiding. The fifth component, control activities, is about procedures and policies. Information & communication have the purpose of collecting, interpreting and communicating information that concerns the organization. Finally, the monitoring, which should be evaluated and adapted regularly, whenever needed.

Figure 4: Enterprise Risk Management - Integrated Framework (Frigo & Anderson, 2011)

4.3 Differences Between the Frameworks

Even though the IC Framework and the ERM Framework can be perceived as similar, Romney and Steinbart (2015) mention that the ERM Framework and the IC Framework have some differences between them. The primary difference is that the ERM Framework have a risk-based approach and the IC Framework is control-based. Besides from the obvious change from five dimensions (IC Framework) to eight dimensions (ERM Framework), the ERM Framework is claimed, by Romney and Steinbart, to be more flexible. This flexibility is claimed to lead towards more relevance in the organization's current objectives.

Romney and Steinbart (2015) furthermore claim that one of the advantages with the ERM Framework is its risk acknowledgement. Acceptance, avoidance, diversification of, sharing and transferring as well as controlling the risk is acknowledged by the ERM Framework. Which means that the model is more extensive in including perspectives.

4.4 ERM Critique

ERM has gotten some critique from Bromiley et al. (2015), who amongst other things have mentioned that the empirical literature on ERM has been slow to address concepts of the core practitioners. This means that some of the terms used within ERM has not yet been properly defined. Furthermore, they mention that research has not yet made it possible to draw

conclusions about how efficient ERM actually is nor has it properly investigated differences that occur inter-firm. Bromiley et al. also critique the extensive focus that research previously had on a micro approach regarding risk management.

Another critique that ERM has gotten is presented by Power (2009), who suggests that risk management provides a false sense of security. Power furthermore claims that risk management have limitations as a platform for institutional re-building and that managers need to understand this issue. Moreover, COSO's ERM has also gotten critique about not including stakeholders' objectives and influence into account when calculating risks (Marks, 2011). Marks also mentions that the risks identified are mostly internal risks, even though external factors are voiced.

4.5 ERM in Public Sector

Baldry (1998) describes that organizations within the public sector have a wide mix of stakeholders, and are thereby target for multiple influences and expectations from several internal and external parties. Further, he argues that the competence and motivations of these stakeholders can improve the risk perception, by widening the perception of risk identification, and thereby improving the risk management. Additionally, the interests of the various stakeholders might differ remarkably, resulting in conflict.

Hofmann (2010) reports that differences in ERM are not dependent on whether it is within public or private sector, but instead rooted in the nature of the entity or industry. Instead the ERM-process are the same within both public and private organizations. However, Hofmann presents that the risk context, as well as the risk content, differs between public and private sector, which might affect how ERM is implemented. For instance, in the private sector ERM is about survival, protecting value and giving competitive advantage. In comparison, ERM in public sector organizations includes protection of citizens and the infrastructure.

4.6 Chapter Summary

COSO released an IC Framework in 1992, which was updated in 2013, due to the globalization, complexity of rules and changing business models. The framework consists of five components namely: control environment, risk assessment, control activities, information & communication and finally monitoring activities. Further, COSO developed the ERM Framework in 2004 in order to create a benchmarking method for organizations. It consists of three dimensions; firstly risk and control elements, secondly it includes four objectives and lastly the dimension of internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication and monitoring. The main difference between these two frameworks is that the ERM Framework have a risk-based approach and the IC Framework have a control-based approach.

The critique against ERM includes lack of properly defined terms, it provides a false sense of security, it does not include the stakeholder and its efficiency has not yet been identified. It is reported that differences in ERM is not dependent on the sector, but instead the industry or entity. Further, organizations in the public sector have a wide mix of stakeholders and thereby receives influences and expectations from several parties. Baldry (1998) describes that this can have a positive effect on the identification of risks. However, it can also create conflicts.

5. Empirical Foundation

The empirical foundation presents the results from the interviews as well as from the documents that have been studied. The chapter starts with the results from the private sector, dividing the answers in themes. The public sector's answers follow the same layout.

5.1 Private Sector

5.1.1 About the Companies

Company 1 was founded in late 19th century and is based in Sweden but work globally with production. They have offices in 18 countries and their vision is to improve the safety and traffic environment. Also, they employ more than 2 000 individuals and have a turnover around SEK 4.8 bn. The company has been listed on Nasdaq Stockholm since late 1980's.

The second respondent, Company 2, was founded in early 20th century in Sweden and is a production company. It employs about 16 000 individuals around the world and operate in 40 countries. Their vision is to be the first choice of their customers in their market segments by creating value with their high-performance solutions. The turnover for the group is around SEK 25 bn and it got listed on Nasdaq Stockholm late in 1980's.

5.1.2 Definition of ERM

In the annual report Company 1 defines internal control as "*a process that is regulated by the Board of Directors and the Audit Committee and performed by the President and Group Management*" (2015, p. 76). In addition, the interviewee stated that ERM is a natural part of the organization and is mainly about identifying, monitoring and balancing the existing risks and then making choices based on the risk assessment.

Company 2 explains that ERM is a process of managing risks within the Group. Moreover, they say that "*this is not something new and it has existed for a long period, even though it might not always have been referred to as ERM*". In their annual report they declared that the

ability of identifying, evaluating, managing and monitoring risks are of importance to the management.

5.1.3 Framework

The COSO Framework has been used by both companies for a long period. Initially, the IC Framework from 1992 was used. However, when the version of 2013 was published, Company 1 thought that there was a reason behind this, since the conditions and environment have changed extensively. As a consequence, both companies implemented the version of 2013. All the groundwork and preparation of the transition to IC Framework 2013 were done by Company 1 itself. Nonetheless, external consultants have held workshops in order to stimulate a dialog and give input. In terms of Company 2, they view that the practical work of risk management have not drastically changed, since the integration of the updated Framework. However, they mention in their annual report that they have a well-developed ERM process in the organization as well.

5.1.4 Who Works with ERM?

Company 1 do not have a single department solely focusing on risk management. Nevertheless, the different types of risks, financial, operational and legal, are handled by different divisions depending on the type of risk. Even though there are still employees that are more responsible of certain risks, and working actively with those. Company 1 describe that risk management is performed in different levels within the organization and it is usually performed on an annual basis. As a result, the work is not only managed vertical from the top down, but risks are also identified in the local entities and then communicated upstream. Furthermore, it is clearly stated that the board of directors are responsible of internal control. Moreover, the board use the audit committee, who have even more extensive instructions. Thereafter, the work is channelled to different functions depending on the type of risks needed to be assessed and controlled. Company 1 exemplified the importance of developing awareness of the tools and frameworks in order to be more proactive. It is not stated in the financial statement either who works with the risks within the organization. However, in the

section about risks and risk management, they state what policies and/or actions they have towards each risk, which concerns different units in the company.

In comparison, Company 2 have an ERM-board consisting of six employees with different background in order to manage the risks. In addition, the risk manager interview each business unit director on an annual base, which was confirmed in their financial statement. Company 2 explained that during this interview, the risks for the specific unit are discussed and documented, as well as the actions taken. Furthermore, the company also perform a risk mapping over all legal entities, which was mentioned in their financial statement as well. Company 2 further explained that this ranking is based on several different parameters. The parameters are unitized and show what companies to focus on when considering to acquire another company. The annual report states that this can lead to different actions depending on how the risk is perceived, which the interviewee also confirmed.

5.1.5 The Work of ERM

In the annual report of Company 1, three different groups of risks are presented; operational, financial and legal risks. Each risk is described and policies and actions taken are presented. The focus in the annual statement is equally divided between operational and financial risks, but only mentioning two legal risks. Although, it is stated that the presented risks give an overall picture and have been fairly consistent for the last four years. Company 1 explain that after a risk has been identified, the company choose whether they should continue or not, depending on how the risk is perceived. If an action or improved monitoring is necessary, they further investigate the routines of the process and then finally decide what action to take. Additionally, the audit committee regularly investigate and improves the policies. The company mean that the organization continuously changes, and thereby should the policies do the same.

From a management perspective Company 1 asses the risks continuously. On the other hand, further down in the organization it is handled in certain cycles. The interviewee states that even though it is important to take an overall approach of the risks, it is sometimes preferable

to investigate more deeply in a certain area. The discovered risks are ranked by probability and consequences.

Company 2 mainly focuses on operational risks, and do not consider their organizations to have many financial risks. They argue that this is due to the structure of the company, a relatively large group consisting of several minor companies. The interviewee explains that a loss in one company is not really affecting the entire Group, why more focus is put on operational risks. However, in the annual report, the company present nine large risks in five areas. For each risk they present information about established key processes and initial and ongoing activities. The financial risks are presented separately from the, previously mentioned, nine large risks. These are risks, which might result in damage and loss with significant impact on the entire Group, and therefore need to be handled at Group level, according to the annual report. They have not changed a lot the last years, since this is, more or less, what their business environment looks like.

A common response to the risks are internal education, since the company usually are aware of how to minimize risk. The problem is usually to educate more employees further down in the organization. Both to make them aware of the issue, but also to understand how to identify a risk and how to respond. Company 2 further explained the importance of authorization, namely to state what you are allowed respectively not allowed to do. Moreover, since the company continually buys companies, it is significant to make the employees in the new acquisition aware of the view and rules concerning risks.

5.1.6 Impacts of ERM

According to Company 1, ERM can only be viewed as something positive, since it creates good dialogs among the functions, enabling the organization to improve and grow. On the other hand, the employees were first worried that the change to the IC Framework of 2013 would lead to increased administration and documentation, since they now had to work with 17 principles instead of the five components. However, the framework was not perceived more burdensome than the old version, only different documentation. Company 1 commented

that several employees perceived the questions as favourable, by enabling them to take a stand regarding where to position the company and how to rank the risks.

Neither Company 2 could see any major disadvantages of using ERM. Nevertheless, they discuss the importance of being aware that it is impossible to identify all risks. Additionally, the company report that they have a good dialog within the organization.

	Company 1	Company 2
Definition of ERM	Identifying, monitoring and balancing the existing risks and then making choices based on the risk assessment.	A process of managing risks within the Group
Framework	IC Framework 2013	IC Framework 2013
Who works with ERM	- Different divisions depending on the type of risk. - Board of directors is responsible of internal control.	- ERM-board - The risk manager performs interviews with each business unit's director regarding risks.
The work of ERM	- Risks are assessed continuously or annually. - Lists operational, financial and legal risks. - The annual report contains descriptions of the risks and suggest actions.	- Focuses mainly on operational risks due to their organizational structure. - A common response to the risks is internal education - Presents nine large risks within five different areas and reports financial risks in a separate sections.
Impacts of ERM	- Creates good dialogs between the departments. - The updated version were not perceived more burdensome	- They have a good dialog within the organization. - Could not identify any major disadvantages.

Table 2: Summary of private sector organization answers

5.2 Public Sector

5.2.1 About the Municipalities

Municipality 1 is located in Scania and it belongs on the top 10 of the largest municipalities in Sweden (Wikipedia, 2016). Almost 15 % of the land is a population centre and about 75 %

is arable land. About 25 % of the population work in another city and the inhabitants mostly vote right-wing politically.

Also located in Scania, is Municipality 2 and it is placed among the 80 largest municipalities in the country (Wikipedia, 2016). More than 60 % of the land in the municipality consists of arable land, while only about 15 % is a population centre and most of its inhabitants commute to other areas to work. Politically, the inhabitants vote right-wing.

5.2.2 Definition of ERM

Municipality 1 does not define ERM, but defines risk management as *"everything that can affect the vision of the departments and the state owned companies"*. Furthermore, it is argued that their operation is spread, why the definition of risk management can vary within the organization. However, the basic view according to their annual report, is that every state owned company is responsible for their own work with risk management.

Likewise, Municipality 2 has a broad definition of risk management but no definition for ERM. The interviewee argued that risk management *"helps to make the organization more efficient, which is the main reason working with this"*. If the organization do not have enough internal control, the politicians will not be granted discharge. Finally, internal control are supposed to be seen as a natural part of Municipality 2.

5.2.3 Framework

Neither of the municipalities use any of COSO's Frameworks in order to prevent risks. Municipality 1 uses a framework called Multidimensional Business Analysis. Since it is impossible to identify all unwanted scenarios, the ability to control risks must be developed and improved. In the framework, there is major focus on vulnerability analysis. Additionally, it includes traditional risk analysis, where probability and consequences are interacted. In Municipality 1's annual report, there is nothing mentioned about what framework is being used, though it is mentioned in the vulnerability analysis report.

In comparison, Municipality 2 argues that COSO was not perceived as an alternative. They mean that the supervision should not be mixed with internal control, because it should be used as a tool to make sure that the operations are working. They describe that they have had consultants arguing that internal control should be a part of the governance, but Municipality 2 do not agree. Instead they use their own framework, a risk assurance analysis, for internal control and risk management. They mention in their annual report that their internal control plans are based on this framework.

5.2.4 Who Works with ERM?

Compared to the private sector, the public sector has an extensive amount of stakeholders, meaning, many actors having opinions. Furthermore, Municipality 1 state that they are responsible for everything that happens in the municipality. They have a wide range of services, from libraries to schools and infrastructure. Even though they are self-governing, there is a major set of rules they need to comply with. The respondents claim that consequently, a company is able to make faster decisions compared to a public organization.

Within Municipality 1 there is no department alone working with risk management. Instead, every department and company are working with some type of risk management. This is done by different degrees and quality. Moreover, the politicians only decide the amount of resources each department are given. By increasing the resources, an opportunity to improve the risk management, is given. Nevertheless, the interviewees explain that the departments usually do not invest the extra resources in risk management.

Likewise, the work of risk management is spread across the organization in Municipality 2. They have several employees working with internal control. Additionally, they have outsourced their financial department, where one person is responsible of the internal control in the municipality. According to their risk assurance analysis, the city council has the main responsibility to ensure that a good internal control exists within the organization. However, each department is responsible of maintaining good internal control within respective area.

The respondents perceive that risk management is not on the top of the agenda within Municipality 1. They mean that the departments already have enough work. Furthermore, they declare that the outcome is highly affected by how it is pitched, as well as the support it receives. The respondents prefer that the municipality should add risk management as one of the main pillars of the organization, besides economy and employees. Additionally, the municipality have developed policies. However, the interviewees reported that since there are no consequences if someone breaks them, there is a risk that employees might not follow them. Moreover, the interviewees argue that most of the risks occur due to humans. They claim that behavioural issues are essential for the organization.

Municipality 1 perform a Risk and Vulnerability Analysis, according to the rule, every fourth year which is revised annually. The report is divided by different areas within the organization where risk scenarios are presented. The framework of the risk analysis is based on a quantitative judgement. Meaning that scenarios are identified and graded based on probability and consequence. After that, actions are identified to minimize the risk, either by reducing the probability or the consequences. The interviewees explain that the highest ranked risks, in either probability or affect, are the ones that are further proceed with. Moreover, it is explained that it is a long process, since they have to convince a large amount of people, of the benefits by taking action against the risks. There is no state overall procedure of how this should be done for each core business. Instead, a dialog is performed with each department. If there is no possible action to prevent a risk, insurance is used. Nonetheless, this is not a preferred action according to Municipality 1. Another outcome of risk management could be that the risks are accepted, because there are not enough resources available.

In the annual report of Municipality 1, there is a varied degree of information about risk and risk management. For their fully-owned companies there are risks identified and for some, controls presented. Furthermore, they list financial risks for the municipality, where the potential consequences are reported and targets are set. These targets are not allowed to be exceeded. Additionally, they publish the risk and vulnerability analysis, were risk scenarios

regarding several different areas, except the financial, are presented. However, there are no possible controls presented.

Municipality 2 perform a risk assurance analysis on an annual basis. The purpose of the report is to identify potential risks, that might prevent the departments from achieving their goals. It consists of four steps, firstly to map the county councils budget responsibility for different areas and important main processes within those areas. In the next step the probabilities and consequences are estimated. Thirdly, the processes that are graded the highest should be prioritized, and selected as control areas in the county council's internal control plan. Finally, based on the risk assurance analysis, audit areas are chosen within the processes that received the highest scores. Thereafter, an internal control report for the county council is developed. As a result, this document provides guidelines of which internal control projects that should be continued.

Furthermore, Municipality 2's annual report contains limited amount of information about risk management. They present some financial risks, but no potential controls or actions. Nonetheless, in the risk assurance analysis they have a more extensive presentation of risks, where categories as; financial, legal, operational, financial reporting, IT and trust is included. Moreover, the document contains information about the probabilities and the consequences for each risk.

5.2.6 Impacts of ERM

Municipality 1 claim that if the work is done correctly, there is high probability that the organization's goals are achieved, and that serious events affecting the organization are avoided. If this is done continuously and systematically, it enables a good overview of the organization. Furthermore, Municipality 2 respond that risk management gives an indication that the organization is efficient, routines are working and that the services are good for the citizens.

On the other hand, Municipality 2 view that there could be a defect in the process, if you do not have a plan that is independent, of those responsible of the organization. Meaning that if

there is a single employee making all the decisions, there is a risk that he withholds areas that needs to be examined. However, since Municipality 2 have outsourced their financial department, they argue that this risk is minimized.

	Municipality 1	Municipality 2
Definition of ERM	- No definition of ERM. - Though, risk management is defined as everything that can affect the vision of the departments and the state owned companies.	- No definition of ERM. - Though, risk management helps to make the organization more efficient.
Framework	- Multidimensional business analysis	- Risk assurance analysis
Who works with ERM	- Every department and company are working with some type of risk management.	- City council are responsible to ensure that a good internal control exist within the organization. However, each department is responsible of maintaining a good internal control within respective area.
The work of ERM	- Performs a Risk and Vulnerability analysis each fourth year but is reviewed annually. It lists risk scenarios. - The annual report presents risks and controls for the state-owned companies and financial risks for the municipality.	- A Risk assurance analysis is developed annually, which contains a more extensive presentation of risks of other categories. - The annual report includes identified risks but no suggestions of controls.
Impacts of ERM	- Goals are achieved, serious risks are avoided and gives a good overview of the organization.	- A risk for subjective judgements. - Shows if the organization is efficient, routines are working and if the services are good for the citizens.

Table 3: Summary of public sector organization answers

6. Analysis and Discussion

An analysis of the empirical findings will be performed, introduced with the same theme as when presenting the empirical findings. The findings will also be discussed in the chapter.

6.1 Definition of ERM

Along the study it was identified that even though Company 2 have an ERM board, they use the IC Framework and not the ERM Framework. However, ERM is only briefly mentioned in the financial statement. Moreover, both companies were asked questions regarding ERM, and neither of them reacted, even though they use the IC Framework, and not the ERM Framework. Consequently, this might indicate that ERM is considered a synonym to internal control. Moreover, a confusion of the different terms could also be traced within Municipality 1. They presented that they were not consistent in their use of terms regarding risks, when pitching ideas of improvements and actions to take. As a result, they explained that their work might not always be considered risk management. Furthermore, they argued that by using the term risk management, other departments might take the actions more seriously and will be more determined to fulfil them. Municipality 2 also adapt a broad view of risk management. They argue that the concept makes the organization more efficient.

Additionally, the definitions of risk management and ERM where different within the organizations. Even this shows how the terms can be perceived variously by different organizations and sectors. Nevertheless, this is confirmed by Bromiley et al. (2015), who state that some terms within ERM has not been properly defined. Most likely, the lack of a clear definition can create confusion within the organizations.

It could also be interpreted that the organizations do not have enough knowledge about what differences there are between the frameworks. As Romney and Steinbart (2015) consider the ERM Framework to be more adaptive and flexible, which might not be known in the organizations. It could be speculated that since COSO has developed and released both frameworks, they might not have done a good job with separating the purpose and aim of the frameworks. As a consequence, companies might select the IC Framework because it is the

most recent framework. Also, due to internal control being mandatory according to the law, the IC Framework might be the most natural choice to the companies in general.

6.2 Framework

Different frameworks are used within the public and private sector organizations. Both companies uses COSO's IC Framework and have done so for a long time. The framework is in accordance with the Swedish Companies Act. The legitimacy theory (Deegan & Unerman, 2011) describes that organizations work in order to be perceived as legitimate by the society. Most likely, the work with risk management is a way of increasing the legitimacy of the organization. For instance, both companies explain that the use of the IC Framework is based on it being a world accepted framework for internal control. Consequently, the IC Framework can be seen as a legitimate framework according to the companies.

However, the municipalities use different frameworks. Municipality 2 argued that COSO was not something they preferred, since they do not believe that supervision should be mixed with internal control. Nevertheless, many steps from the ERM Framework can be identified within the municipalities. For instance, both municipalities claim that risks are being identified and ranked and that some risks are accepted. Furthermore, they both have developed policies and clearly stated at what level the responsibility of internal control is put. Moreover, they present actions that are taken in order to minimize or prevent risks. This indicate that parts of the ERM Framework can be traced within the public sector. An implementation of the ERM Framework could therefore be considered as a not too drastic step for the municipalities.

The question of why the municipalities do not use either of COSO's frameworks still remain. Instead of using a framework that is internationally recognized and accepted, Municipality 1 use Multidimensional Business Analysis and Municipality 2 use their own composition as a framework. Therefore, it could be considered that the municipalities have created a legitimacy gap (Sethi, 1978) by not using any of COSO's frameworks. One reason might be that the stakeholders (Deegan & Unerman, 2011) do not put pressure on the municipalities to use a more legitimate framework as long as any internal control is being used. Or perhaps it depends on the fact that neither of the municipalities have hired consultancy firms regarding

risk management? For instance, Company 1 hired a consultancy firm in order to implement the updated version of the COSO Framework. Company 2 on the other hand, has an ERM board that is dedicated to the work around the company's ERM and internal control. This have most likely eased the work with ERM in the organizations, or at least eased the introduction of it. Another possible explanation could be that the organizational structure are remarkably different between public and private sector. Which would mean that the difference between the organizations are too extensive and therefore, COSO's Frameworks are not in compliance with the municipalities structures and directives. Further, the reason for the different organizational structures could be due to the municipalities already having more rules to comply with. The municipalities also have a longer decision-making process, which might aggravate the ability of using COSO. Moreover, if the responsibility of internal control and risk management is more spread across the organization, it might be hard for the organization to get an overview of the changes, without having someone specifically responsible.

6.3 Who Works with ERM?

Both companies described that risk management has been a natural part of the organizations for a long period. This was confirmed when studying their annual reports over the last years. Consequently, this can be viewed as a clan control (Malmi & Brown, 2008), where the organization making sure that risk management is included in the mind-set of all employees. It could also be viewed as Simon's (2000) belief system. However, this is not the case in Municipality 1, who describe that risk management is usually not prioritized. Nevertheless, they stated that they want risk management to be included in the organization's main-pillars.

It was not clear which employee should answer the interview questions in Municipality 1. When first contacted, several employees considered themselves to be the wrong respondent, thus recommending someone else to interview. This indicates that the municipality have not clearly expressed who is responsible for risk management. Nonetheless, both municipalities have several documents presenting at what level the responsibility for internal control is put. This can be viewed as what Malmi and Brown (2008) calls administrative controls, which clarifies to whom employees should be held accountable for its behaviour. However, the

responsibility of internal control might not either be as clear in reality as the documents indicates. Consequently, the work might be done with different quality within the organization, making it harder to review. In comparison, the responsibility of risk management was clearer within the companies, which shows that the business environments are remarkably different between public and private sector. This contradicts Hofmann (2010), who stated that the differences did not depend on the sector, but rather on the nature of the industry or entity.

6.4 The Work of ERM

Another finding that supported the different business environments, are the various stakeholders (Knutsson et al., 2006) that exist between public and private sectors. However, it can be argued that there is a greater variety of interests among the stakeholders in the public sector, since a municipality provide multiple services. Furthermore, the result showed that municipalities present more various risks compared to the private organizations, which might be explained by municipalities offering more services and acting in different conditions and environments (Hofmann, 2010). The municipalities are structured different compared to private organizations and the decision-making process is longer. Moreover, the work of risk management is more spread within the municipality, since the responsibility is channelized to each company and department, especially in Municipality 1.

When comparing the private sector organizations towards public sector organizations, the applicable systems that Simon (2000) mentions, shows difference in focus. This difference is also occurring in the annual reports and other documents. However, the municipalities considers a wider range of risks than the companies, which most likely can be explained by their extensive responsibility of everything that happens within the municipality's border and their broader scope of services.

Based on the study it was found that all organizations perform risk management and continuously identifies risks. However, the presented risks are quite similar and consistent over the years. This can be based on the fact that the business environment are not affected by any major changes, which was confirmed by Company 2. Furthermore, all organizations rank

their risks using the parameters probability and consequences. As a result, there is several similarities in the use of risk management within the public and private sector.

The controls of the financial risks that are presented in all respondents annual reports can be labelled diagnostic controls (Simon, 2000), since controls are implemented if the maximum target is exceeded. Moreover, it was discovered that the municipalities only list diagnostic controls in their annual report, since only financial risks and controls were presented. Nevertheless, they publish other documents containing more operational risks.

However, three out of four respondents presents the financial risks separated from other risks. The question is why? One reason could be due to researchers mainly looking in the financial statement and that the organizations also have confidential documents that was not accessed. Another reason could be that the impact of financial risks are perceived to have more serious effects on the organization, thus wanting to separate them from the other risks. It might even be due to the cultural control, that traditionally financial risks have always been separated from other risks (Malmi & Brown, 2008).

Whether the controls and actions mentioned in the organizations' documents are followed or not, is hard to get a picture of. All respondents have knowledge about risk management which they share during the interview. Company 1 have a lot of information regarding their risk management in their financial statement, as does Company 2. Furthermore, Company 2 share their view on ERM and internal control on their webpage to make it more accessible to its stakeholders (Deegan & Unerman, 2011). Municipality 1 talk about controls and actions a lot during the interview, but rather little of that information is shared in the financial statement and other documents. Mostly, that information is limited to its fully-owned companies. Municipality 2 states that they do not wish for the internal control to put a strain on the organization, that enough is enough. Though, they release complementary documents regarding the internal control of the municipality.

6.5 Impacts of ERM

The study demonstrated that the overall view of risk management was positive. The organizations describe that risk management can help to achieve the organization's goals. Risk management can therefore be seen as long-term action planning (Malmi & Brown, 2008), since it enables the organization to take a more strategic focus. Furthermore, by minimizing or eliminating risk scenarios, there is a greater probability that the organization's goals will be achieved. Municipality 2 described that risk management indicates whether the organization is efficient or not, routines are working or that the services are perceived as good for the citizens. However, as Power (2009) argue, risk management can provide a false sense of security. As a result, this dominated positive approach might deceive the organization to feel too secure and thereby missing major serious risks.

Both companies view risk management as a tool that improves the communication within the organization, which is in accordance with Simon's (2000) belief systems respectively boundary systems. These systems emphasize good communication in an organization, which can be in the shape of company's values respectively risks to avoid. Both of these systems are required for an organization in their strive for developing and controlling the company. In comparison, the public sector indicates that risk management evaluates if the organization is efficient, achieves their goals and also gives an overview of the organization. This could be connected to Simon's diagnostic respectively interactive systems, which emphasizes, among other things, measuring respectively uncertainties in the organization. These systems are also examples of necessities within an organization.

It is likely that the use of risk management and internal control is about the administrative control systems (Malmi & Brown, 2008). The system helps directing employee behaviour by organizing, monitoring, establishing codes of conduct and clarify to whom the employee should be held accountable for its behaviour. Which can be interpreted as if someone specific is made responsible for the company's risk management, it would become easier for the company to follow up on the development in the area. Company 2 is the only organization that have a specific department for its ERM. If deemed necessary, the other organizations

could easily implement this in their own organizations. Which, if implemented, could have a positive effect on the organization.

Furthermore, the cultural controls (Malmi & Brown, 2008) also affect an organization and its development. If top management in the organization considers ERM be of great value for the organization, and support the use of it, prioritizes it, then it is likely that employees would start consider the framework more important. Thus, letting ERM having a greater impact on the organization. Which is something that Company 2 have done by creating an ERM board, showing the stakeholders (Deegan & Unerman, 2011) what the company prioritizes.

6.6 Chapter Summary

Definition of ERM	- ERM might be considered a synonym to internal control - The organizations' definition of ERM and internal control were different. - The municipalities did not define ERM but risk management. - The organizations have most likely not enough knowledge about the differences between the frameworks.
Framework	- The COSO Framework can be considered legitimate. - Several steps in the COSO Framework can be identified within the municipalities, why an implementation of the framework would not be too drastic. - The reason why the municipalities do not use COSO might be that their stakeholders do not require it or because they have not hired consultancy firms.
Who works with ERM	- Risk management have been a natural part of the organizations for a long period, and can thereby be viewed as clan control. - Even though the municipalities have several documents clarifying the responsibility of internal control (administrative controls), the responsibility might not be as clear in reality.
The work of ERM	- The presented risks are similar over the years, which might be a result of a stable business environment. - Municipalities only list financial risks (diagnostic controls) in their annual report, compared to the companies who presents all risks.
Impacts of ERM	- The dominated positive view on risk management might deceive the organization to feel too secure and thereby missing serious risks. - The private sector view risk management as a tool that improves the communication (belief and boundary systems). - According to the public sector, risk management is a tool for measuring the organization's efficiency (diagnostic and interactive systems).

Table 4: Summary of analysis

7. Conclusions

The findings from the analysis and discussion is being presented and summarized in major points of the thesis and suggestions for future research will be mentioned.

7.1 Major Points

The aim of this study was to contribute to the knowledge on the use of risk management and ERM in different contexts. The data is broadly consistent with major trends in the literature as to no uniform definition of ERM was found. Instead, each organization have their own definition and take different approaches when working with risk management. Moreover, the study has indicated that a confusion of the terms ERM and internal control exists, since they were used as synonyms. Further, it was found that working with ERM was perceived as positive and all respondents viewed risk management as a necessary part to include in the organization. Consequently, the definition of ERM is most likely not crucial for working with risk management.

Further, it was found that risk management is performed very differently between public and private sector. It was shown that companies and municipalities uses different frameworks, focuses on different types of risks and the work is performed at different levels. These results concur with other studies that show that differences in ERM are dependent on the industry or entity and not the sector the organization exists in. However, previous literature states that the purpose of ERM is different between the public and private sector. This is consistent with the finding of this study, since the municipalities and companies take different approach and focus when identifying risks. The risks the companies present contain occurrences threatening the company's future. In comparison, the municipalities had a higher focus on the citizens' safety as well as the infrastructure of the city.

The study demonstrates that all respondents perform risk management despite their different stakeholders. This indicates that the stakeholders are not affecting whether an organization use ERM or not. However, as previous research states, the different stakeholders will most likely affect the work of risk management. For instance, if the stakeholders are not aware of

or interested in risk management, there is a risk that the internal control might not be complied with.

Even though the municipalities talked about what controls and preventative actions they implement, few indications were found in their documents, to support their claim. Neither could the delegation of responsibility, stated in the documents, be identified during the study. Thus, the conclusion was made that the municipalities have a hard time to practice as they preach. Further, it might be more natural for municipalities to talk about controls and risk management, and write it down as policies and procedures, than performing actions. A reason might be the political climate or the transparency required in the organizations.

7.2 Suggestions for Continuing Research

Previously, the research on ERM was limited and there was a clear gap in knowledge concerning the variation in the use of ERM between and within different organizations. Indications have been found regarding municipalities not practicing as they preach. Furthermore, it has been confirmed that definition of ERM is not of importance for the organizations' work with risk management. Another indication found, regardless of conditions and stakeholders, organizations work with risk management.

However, several questions remain to be resolved, in particular it would be interesting to further investigate the definition of ERM, since this study could not clearly state a single definition. Whether a municipality would benefit from the use of the ERM Framework and in that case, how it would benefit is also interesting topics for future research. Does companies use the IC Framework due to convenience or because it is the most recent framework that COSO has released? Is the difference between the ERM Framework and the IC Framework clear enough or does COSO need to clarify it more for organizations to understand the difference? Since the ERM Framework is considered to be more flexible as a framework and have a broader overview, how come it is not being used more? Another research topic could be finding out what it would take for a municipality to start implement a full version of COSO's Framework. Finally, it would also be interesting to find out if the indications found in this study would last in a more extensive study or if the result would be different.

7.3 Chapter Summary

The aim of the study was to contribute to the knowledge on the use of risk management and ERM in different contexts. The study found indications of confusions concerning ERM and internal control both in the public sector organizations as well as the private sector organizations. Further, it was found that the work with risk management did not depend on the organization's stakeholders. Also, indications were found regarding principles and processes being hard to implement in reality. Finally, it was confirmed that regardless of what definition an organization had, they all worked with risk management of some kind.

Some of the suggestions left for future research include researching if a municipality would benefit from the use of ERM and how? Also, finding out what it would take for a municipality to start using a COSO Framework. The final suggestion concerns this study and if the results would remain in a more extensive study.

References

Abernethy, M. A. & Chua, W. (1996). Field Study of Control System 'Redesign': the Impact of Institutional Process on Strategic Choice. *Contemporary Accounting Research,* vol. 13, no. 2, pp. 569–606

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: en handbok*. Stockholm: Liber, 2013 (Kina)

Baldry, D. (1998). The Evaluation of Risk Management in Public Sector Capital Projects. *International Journal of Project Management*, vol. 16, no. 1, pp. 35-41

Bonner, S. E. & Sprinkle, G. B. (2002). The Effects of Monetary Incentives on Effort and Task Performance: Theories, Evidence, and a Framework for Research. *Accounting, Organizations And Society*, vol. 27, no. 4-5, pp. 303-345

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015), Enterprise Risk Management: Review, Critique, and Research Directions, *Long Range Planning*, vol. 48, pp. 265-276

Bryman, A. & Bell, E. (2013). *Företagsekonomiska Forskningsmetoder*. Polen: Liber AB

Bryman, A. & Bell, E. (2015). *Business research methods*. Oxford: Oxford University Press

Clarkson, M. E. (1995). A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance. *Academy Of Management Review*, vol. 20, no. 1, pp. 92-117

Company 1 (2015). Annual Report.

COSO (2004). COSO Releases Enterprise Risk Management – Integrated Framework [pdf]. Available at: http://www.coso.org/documents/PR_9-29-04_ERM-IntegratedFramework.pdf [Accessed 19 April 2016]

COSO (2013). Internal Control - Integrated Framework - Executive Summary [pdf]. Available at:

http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf [Accessed 20 April 2016]

Courpasson, D., & Reed, M. (2004). Introduction: Bureaucracy in the Age of Enterprise, *Organization*, vol. 11, no. 1, pp. 5-12

Deegan, C. & Unerman, J. (2011). *Financial Accounting Theory*. Maidenhead: McGraw-Hill Education

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance. Issues and Practice*, vol. 26, no. 3, pp. 360-366

Faris, C., Gilbert, B., LeBlanc, B., Ballou, B. & Heitger, D. L. (2013). Thought Leadership in ERM. Demystifying Sustainability Risk [pdf]. Available at: http://www.coso.org/documents/ COSO-ERM%20Demystifying%20Sustainability%20Risk_Full%20WEB.pdf [Accessed 19 April 2016]

Flamholtz, E. G. (1983). Accounting, Budgeting and Control Systems in Their Organizational Context: Theoretical and Empirical Perspectives. *Accounting, Organizations & Society*, vol. *8,* no. 2/3, pp. 153-169

Freeman, R. E. 1984. Strategic management: A stakeholder approach. Pitman: Boston.

Freeman, R. E. & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, vol. 25, no. 3, pp. 88-106

Frigo, M. L. & Anderson, R. J. (2011). Embracing Enterprise Risk management - Practical Approaches for Getting Started [pdf]. Available at: http://www.coso.org/documents/ EmbracingERM-GettingStartedforWebPostingDec110_000.pdf [Accessed 21 April 2016]

Hofmann, A.M. (2010). ERM Basics Same Across Sectors. *Business Insurance*, vol. 44, no. 41, p. 11-14

Hood, C. (1995). The "New Public Management" in the 1980s: Variations on a Theme. *Accounting, Organizations & Society*, vol. 20, no. 2/3, pp. 93-109

Håkansson, V., Jakobsson, M. & Lundin, M. (2015). COSO-Ramverket Inte Enbart Ett Intern Kontrollverktyg i Företagsvärlden - En Flerfallstudie Inom Den Kommunala Sektorn, Bachelor Thesis, Department of Business Administration, Lund University. Available online: https://lup.lub.lu.se/student-papers/search/publication/8852508 [Accessed 1 April 2016]

Knutsson, H., Mattisson, O., Ramberg, U. & Tagesson, T. (2006). *God Kommunal Hushållning Måste Man Arbeta För*. Lund: Studentlitteratur (Danmark)

Knutsson, H., Mattisson, O., Ramberg, U. & Tagesson, T. (2008). Do Strategy and Management Matter in Municipal organisations? *Financial Accountability & Management*, vol. 24, no. 3, pp. 295-319

Lapsley, I. (2009). New Public Management: The Cruellest Invention of the Human Spirit? *Abacus*, vol. 45, no. 1, pp. 1-21

Malmi, T. & Brown, D. A. (2008). Management Control Systems as a Package— Opportunities, Challenges and Research Directions. *Management Accounting Research*, vol. 19, pp. 287-300

Marks, N. (2011). 10 reasons not to like the COSO ERM framework – a discussion with Grant Purdy. Available at: https://normanmarks.wordpress.com/2011/02/21/10-reasons-not-to-like-the-coso-erm-framework-–-a-discussion-with-grant-purdy/ [Accessed 2 May 2016]

McNally, J. S. (2013). COSO Framework and SOX Compliance - One Approach to an Effective Transition. [pdf] Available at: http://www.coso.org/IC.htm [Accessed 14 April 2016]

Munck, J. (2014). Sveriges Rikes Lag. Finland: Nordsteds Juridik AB

Neu, D., Warsame, H., & Pedwell, K. (1998), Managing Public Impressions: Environmental Disclosures in Annual Reports, *Accounting, Organizations & Society*, vol. 23, no. 3, pp. 265-282

Ouchi, W. (1979). A conceptual framework for the design of organizational control mechanisms. *Management Science,* vol. 25, no. 9, pp. 833–848.

Palermo, T. (2014). Accountability and Expertise in Public Sector Risk Management: A Case Study. *Financial Accountability & Management,* vol. 30, no. 3, pp. 322-341.

Power, M (2009), The risk management of nothing, Accounting, Organizations and Society, vol. 34, pp. 849-855

PWC (2015). Enterprise Risk Management in the Public Sector [pdf] Available at: https://www.pwc.se/sv/offentlig-sektor/assets/enterprise-risk-management-in-the-public-sector.pdf [Accessed 7 April 2016]

Romney, M. B. & Steinbart, P. J. (2015). *Accounting information systems*. Harlow: Pearson

Schein, E. (1997). O*rganizational Culture and Leadership*. San Francisco: Jossey-Bass

Sethi, S. P. (1978). Advocacy Advertising: The American Experience. *California Management Review,* vol. 21, no. 1, pp. 55-67

Simons, R. (2000). *Performance Measurement & Control Systems for Implementing Strategy*. New Jersey: Prentice-Hall

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy Of Management Review*, vol. 20, no. 3, pp. 571-610

Wikipedia (2016a). Available at:
https://sv.wikipedia.org/wiki/Lista_över_Sveriges_kommuner [Accessed 28 April 2016]

World Economic Forum (2016). *The Global Risks Report 2016 - 11th Edition*. Geneva: World Economic Forum

Yin, R. K. (2014). *Case study research: design and methods*. London: SAGE

Yin, R. K. & Nilsson, B. (2007). *Fallstudier : design och genomförande*. Malmö : Liber, cop. (Slovenien)

Appendix

Main interview questions

    1.Who are you?

    2.What is your role in the company/organization?

    3.What company/organization do you work for?

    4.Within what industry?

5. What is enterprise risk management to you?

6. How is enterprise risk management used within the company/organization?

- Framework? (COSO, own composition of framework)
- How many are working with ERM?
- How long have the organization been active within ERM?
- Why did you chose to work with ERM?

7. Have the company/organization benefited from using/implementing enterprise risk management?

- How?
- What was the expectation before using ERM and how did those expectations change?

8. Have the ways of thinking changed (gaining bigger knowledge/conscience) with using enterprise risk management?

9. How does the company/organization work with enterprise risk management?

10. What negative aspects are there with using enterprise risk management?
- Time consuming, employee consuming?

11. Do you perform enterprise risk management within the organization or hire consultants?
- If consultants, has it been worth the money?