UNIVERSITY OF AGDER

Unveiling barriers and enablers of risk management in interoperability efforts

A study from the Norwegian public sector

Pernille Monstad Røberg

Supervisor

Leif Skiftenes Flak

This Master's Thesis is carried out as a part of the education at the University of Agder and is therefore approved as a part of this education. However, this does not imply that the University answers for the methods that are used or the conclusions that are drawn.

University of Agder, 2013

Faculty of Economic and Social Sciences

Department of Information Systems

Preface

This thesis presents research conducted during the spring of 2013, as a final delivery for a Masters of Information Systems at the University of Agder in Kristiansand Norway.

The aim of this research was to explore enablers and barriers of risk management in public ICT efforts. Working with this thesis has been very interesting, but also challenging. It has been a continuous learning process where I have had the chance to pursue a field I find very interesting

I wish to express my deep gratitude and appreciation to the following, as without them the completion of this study would not have been possible:

The study could not have been completed without the eleven interviewees who gave their time to provide valuable and useful information.

Thanks to my friends who helped reading though the thesis and checking grammar in addition to providing me support through this semester

Thanks to my supervisor, Leif Skiftenes Flak, who provided me with valuable feedback throughout the progression of my work. I thank him for his constructive comments and recommendations.

And finally, a big thanks to my parents for their continuous support, confidence and patience. Without you I could not have done it.

Sandnes, Norway, June 7th 2013

Pernille Monstad Røberg

Abstract

All projects have uncertainty and Risk. Projects under a high risk have a high probability of failing to meet its targets like time, cost, quality and content. It is therefore important to manage it and try to reduce the risk. Risk management is a continuous process throughout the life cycle of a project and is a topic gaining increased attention. Likewise, e-government and interoperability has gained increased attention. Both eGovernment and interoperability projects are by many viewed as complex and challenging undertakings explored with high risks. The term eGovernment has been used to reflect the implementation of ICT in public administration. An important aspect of eGovernment is interoperability. Improved efficiency of service delivery and more efficient decision-making are some of the benefits of interoperability.

My research question is: *What are the barriers and enablers of risk management in public ICT efforts?*

In order to answer the research question, I have reviewed previous literature on risk management and barriers to project risk management with a focus on the public efforts. A qualitative study with a grounded theory approach to analysis was conducted to investigate risk management with eleven respondents in nine organizations. Eight of the organizations are public and the ninth is private. Half of the interviews were conducted face-to-face and the other half over the phone. The results from the study were systemized and categorize using the qualitative research tool Nvivo.

The results of the study show that many public organizations are managing risk. However, the organizations I studied had varying level of experience in managing risk. A number of barriers and enablers were identified and systemized throughout my study. Lack of top management support and lack of understanding are two factors that are emphasized by the respondents as barriers to risk management. Several respondents also pointed out that management should impose requirements and that this will enable risk management and the decision-making process. Having a simple framework with rich description of what to do and how to do it is generally viewed as an enabler. Good communication and ownership is also viewed as enablers of risk management. Interoperability is deemed as challenging and the importance of managing risks increases. It is increasingly important to have a shared perception on risk communication, understanding and clear definition on goals of the projects.

This study contributes to research on the topic of risk management, and contributes to increased understanding and knowledge of risk management in practice related to Norwegian public organizations. The findings of this study are summarized by six barriers and eight enablers to risk management and risk management practice. Organizations adapting risk management or looking to improve their risk management process should strive to reduce the impact of barriers and to exploit and strengthen the enablers to succeed in their work

It is also important to emphasize that the findings are not set answers, but rather a first attempt at a theoretical understanding of issues related to risk management in the Norwegian eGovernment settings. This understanding has implications of what can be done better in practice, and further research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Introduction

During the last few years there has been a shift in the way that public organizations work. The Norwegian government published a program called *"Digitizing public sector services – Norwegian Government Program"* and the aim of this program is to create better and faster interaction with the public, online interaction and to generate improvements across the sector. In 2009 the Agency for Public Management and eGovernment (DIFI) developed a *"project wizard"* that aims to improve public projects and is a model for conducting digitization projects in the public sector. A digitized government can also be called eGovernment. In recent years DIFI have also worked on recommending a risk management standard for the government and in 2012 they made the ISO/IEC 27001:2005 standard, the recommended government standard (DIFI, 2012).

In recent years eGovernment has received increased attention and the importance of e-governance is growing. eGovernment can be viewed as "*the most interesting and dynamic examples of the integration of Information Technology"* (Whitmore & Choi, 2010). Key reasons for ICT investments in governments are according to Flak et al. (2009) *"increased efficiency of government operations, strengthening of democracy, enhanced openness […] and provide better and more versatile service"*. A challenge within eGovernment is measuring the cost and benefits. Another challenge is that e-governance projects are "*full of risk and uncertainties"* (Choudhari, Banwet, & Gupta, 2005). Research focuses on risk factors, but there is little attention to risk assessment framework and e-governance in the literature (Choudhari, Banwet, & Gupta, 2006).

Another important aspect of is interoperability. Interoperability is viewed as something complex and has several definitions. Interoperability can be defined as the ability of two or more systems to exchange information and knowledge. (Jansen & Schartum, 2008; Misuraca, Alfano, & Viscusi, 2011). Another definition on interoperability used by Solli-Sæther and Flak (2012) is *"a company's organizational and operational ability to collaborate with its partners to effectively establish, implement and develop IT-supported business relationships to create value"*. In summary, interoperability is the ability to exchange information between two or more systems. The systems can be IT-systems, citizens, businesses and others.

IT projects have a long history of failing (Bakker, Boonstra, & Wortmann, 2009; Chulkov & Desai, 2005; Kappelman, McKeeman, & Zhang, 2006; The Standish Group, 1994, 2009). According to the much criticized and cited CHAOS report (The Standish Group, 1994), 31% of all IT project in 1994 were cancelled, and 52% of the projects had an average of 189% of budget costs. The projects that finished had between 42% and 74% of the planed functionality. The success rate for IT projects in 1994 was as low as 16,2%. In 2009, the Standish Group published a new comprehensive report, CHAOS Summary, presenting data on the success rate of projects, which was still low, but showed signs of improvement. The success rate in

2009 had gone up to 32%, 24% of projects were cancelled and 44% were delivered either late or over time or budget, or were delivered with less functionality than planned.

Several authors have written about the reasons why IT projects fail. Neimat (2005) points to poor planning, unclear goals and objectives and failure to communicate and act as a team. Carlos (2008) also points to some of the same reasons; Lack of a solid project plan, unrealistic timeframe and tasks, and undefined objectives and goals. The follow-up report to the Chaos report, Unfinished Voyages (The Standish Group, 1996), points to user involvement, good planning and smaller milestones as success criteria for IT projects. Cohn (2006) presents estimation and planning as two essentials to succeed with developing projects and that a good plan should help reduce risk and uncertainty. Kappelman et al. (2006) did an extensive research on reasons for failure and early warning signs and identified a list of no less than 53 ranked reasons for failure. Lack of top management support, requirements and scope not being documented, lack of effective communications and poor project management are only a few of the reasons, which resulted from their work.

Project failure has been a research topic for several years, but still remains challenging. Lately there has been an increase in the focus of risk management in the public sector in both UK and US (Duggan, 2006; Hofmann, 2008). Departments, agencies and other organizations have been asked and advised to report and assess risks in their business. A continuously increasing number of organizations focus on risk and tools like risk matrixes are more commonly used in strategic plans and business plans. We can say that risk management is the new trend in the government. Braig, Gebre, and Sellgren (2011) write that risk management *"often is more difficult for public-sector institutions than for companies"*. Further the authors point to seven challenges specific to the public sector. Some of the challenges are frequent leadership changes, complex procedural requirements and limited risk culture and mind-set (Braig et al., 2011).

According to both Duggan (2006) and Hofmann (2008) the public sector faces a challenge when it comes to risk management. Both authors point to the need for risk management to be included in the business, and not be viewed as a separate thing. Other challenges are that there is *"no firm and fast definition"* and *"Everybody thinks there´s some sort of magic checklist"* (Hofmann, 2008). A third challenge pointed out by Hofmann (2008) is that governments are a bit slow when it comes to implementing new things. The complexity of management and communication within and between public administrations *"indicates the need for structuring risks"* (Walser, Kühn, & Riedl, 2009).

1.1 Motivation

There are several reasons that led to my motivation for choosing Risk Management as a topic for my thesis. Risk Management is a topic that caught my interest early. As a student at the University of Agder (UiA), through the classes IS-304 and IS-407, I was introduced to project management and the importance of project planning. Through a job as project planner I received experience on scheduling and status reporting. During a semester abroad, at

University of Nebraska at Omaha (UNO), I was able to take a class on Project Risk Management, ISQA 8820, and completed a term project on the topic. My interest towards Risk Management has increased and these classes are the contributing factors as to why I want to immerse myself within this topic. I also want to work with risk management after graduation, which further adds to my motivation.

1.2 Problem statement and research question

There has been little research on risk management risk management in the Norwegian public sector and what barriers can be found. DIFI have made some reports on risk management and information security frameworks, but little research point to my chosen topic. To receive a better understanding of barriers to risk management, the following problem statement was chosen for this thesis:

What are the barriers and enablers of risk management in public ICT efforts?

To be able to answer the problem statement in the best possible way, I find it necessary to break it down into four research questions. The following questions are seen as necessary to answer the problem statement:

- *What is risk management?*
- *What is the purpose of risk management and how can it be performed?*
- *What characterizes barriers and enablers of risk management?*
- *What characterizes risk management in interoperability efforts?*

To examine this, I found it necessary to draw on literature from other domains rather than literature presented only from a public sector perspective. I have therefore reviewed several strands of literature related to the public sector, i.e. eGovernment and interoperability, general risk management and risk management related to IT projects.

1.3 Delimitation

This study focuses on the Norwegian public sector, but the scope of the literature review is encompasses the broader IS literature as little research on this topic in the Norwegian public sector exists.

1.4 Thesis Structure

This section gives an overview of the structure used in this thesis. In the second chapter of this study I carry out a literature review. The first part of chapter two describes the context of this study, public sector, including eGovernment and interoperability. The second part of this chapter includes the concepts of risk and risk management, and critical success factors for risk

management. The last part of the literature review includes good practices for risk management and a comparison of different risk management standards.

The third chapter includes methods and techniques used for the study, including a short description of the respondents. The findings from the interviews are presented in chapter four. Chapter five discusses the challenges identified in the interviews and literature. Chapter six includes the conclusions of this study, implications for research and practice.

The report should be read in its entirety and the chapters in the order they are presented to ensure total comprehension.

2. Literature

This chapter presents previous research on eGovernment, interoperability and risk management. The aim is to create an overall understanding of the context and the challenges that can occur, risk and risk management, and how it can affect the public ICT projects. In the first section of this chapter I present previous research on the public sector in regards of interoperability. The concepts of risk and risk management will be presented in the second section. Further, I will present critical success factors and challenges related to risk management both in general and related to public ICT projects. At the end, a summary of previous research is presented.

I have used a structured approach to determine the source of material used in my literature review, as recommended by Webster and Watson (2002). The first step the authors recommend is to search for information in the leading journals, as the major contributions are likely to be found there. I have used research databases such as EBSCOhost, Scopus, ProQuest, Emerald and Google Scholar. When searching on these websites I have used keywords like "risk", "risk management", "interoperability", "eGovernment", "risk and interoperability", "barriers to risk management" and so on. In addition I have used general web searches. The second step they recommend is to go backwards and look at the references in the articles identified in step one. I have used the reference list from most of the articles identified during this research and the reference list from articles used in previous courses. The last step I performed in order to get material for my literature review, was to use curriculum from attended courses at UNO (ISQA – 8820 Project Risk Management) and UiA.

2.1 Public sector

In this section I present the concepts of eGovernment and interoperability.

During recent years we have seen a shift in the way that public organizations work and we have several examples of this in Norway. During spring 2012 the Norwegian government published a new program called *"Digitizing public sector services – Norwegian Government Program"* (Norwegian Ministries, 2012). The program discusses how the government, citizens and other organizations can benefit from a digitized government. *"Norway is to be at the forefront internationally in terms of providing digital public services to its citizens and businesses"* (Norwegian Ministries, 2012). The aim of this program is to create better and faster interaction with the public, online interaction and generate improvements across the sector. Digitization also helps freeing up resources that can be spent elsewhere, creating savings in one area and solving problems in other areas.

As of spring 2013 many of the services provided by the public sector and government are digitized. Examples include the Norwegian Tax Administration and some health care services that are amongst the services that have become more available online as a result of digitization.

Another example of the shift in the public sector was made by the Agency for Public Management and eGovernment (DIFI). In 2009 they developed an online *"project wizard"* which is a recommended project model for conducting digitization projects in the public sector. The *"project wizard"* was commissioned by the Norwegian government in 2008. The goal of the *"project wizard"* was to achieve better coordination and management of large and/or strategically important public ICT projects. The *"project wizard"* is based on both experiences throughout the public sector and the PRINCE2 framework. PRINCE2 stands for PRojects IN Controlled Environments and is a *"method for effective project management"* (PRINCE2, 2013).

The *"project wizard"* is aimed at project managers and project owners and is intended to help improve the ability to implement digitization projects and improve the success rate of such projects. The first version, also known as PW 1.0, was developed in collaboration with a network of participants from approximately 50 agencies and municipalities. This version was a collection of examples of how to implement and conduct good, public ICT-projects. The *"project wizard"* was updated to version 2.0 in December 2012 and is now the general recommended project model for the public sector (DIFI, 2013).

2.1.1 eGovernment

An important aspect within the public sector is eGovernment. In recent years eGovernment has received increased attention and the importance of e-governance is growing. The term "e-governance" has been used more to reflect the implementation of ICT in the public administration to have easy access to governmental information (Information & Security, 2004). There are many definitions of e-governance, and one definition is *"a system to improve and to support a good government through the use of Information and Communication Technology"* (Joshi & Tiwari, 2012). Another definition used by Novakouski and Lewis (2012) is *"the use of information and communication technologies (ICTs) to improve the activities of public sector organizations.* The importance with e-governance is to access information electronically, and to use the electronic information technology to *"break the boundary of administrative organizations"* (Zhou & Hu, 2008).

EGovernment can be viewed as "*the most interesting and dynamic examples of the integration of Information Technology"* (Whitmore & Choi, 2010). Key reasons for ICT investments in governments are according to Flak et al. (2009) *"increased efficiency of government operations, strengthening of democracy, enhanced openness […] and provide better and more versatile service".*

Achieving benefits from e-governance might not be as easy as it looks and it involves more effort than making governmental information available online. An important aspect of eGovernment is *interoperability*, meaning the ability for two or more systems to exchange information and knowledge (Jansen & Schartum, 2008; Misuraca et al., 2011).

2.1.2 Interoperability

Interoperability has multiple definitions and is viewed as a complex problem (Novakouski & Lewis, 2012). According to Gottschalk and Solli-Sæther (2008) interoperability is referring to

"a property of diverse systems and organizations enabling them to work together". Another definition of interoperability used by Solli-Sæther and Flak (2012) is *"a company's organizational and operational ability to collaborate with its partners to effectively establish, implement and develop IT-supported business relationships to create value"*. The commonality of these definitions is that they both relate to the ability of information sharing across borders. The exchange of information can be done between public organizations as well as between private and public organizations (Gottschalk & Solli-Sæther, 2008).

According to Misuraca et al. (2011) *"interoperability is predominantly seen as a means of developing the cross-border dimension of e-Government"*. This is supported by Gottschalk and Solli-Sæther (2008) who writes that interoperability is of critical importance to make eGovernment successful. Novakouski and Lewis (2012) point to increased challenges of interoperability and states that *"interoperability is a barrier to achieving the benefits of e-government"*. They believe that better understanding of the context and issues will resolve difficulties and suggest paying attention on the increased challenges of interoperability.

There are many benefits of interoperability in an eGovernment context. Some of them are improved efficiency of service delivery and greater access to services, more efficient decision making, enhanced transparency and accountability, and the promotion of cooperation by supporting cross-border efforts (Novakouski & Lewis, 2012).

There are three categories of interoperability: technical, semantic and organizational. Technical interoperability relates to data exchange between systems and semantic interoperability relates to exchanging meaningful data between systems. The last category of interoperability, organizational interoperability, relates to that systems can participate in multi-organization business processes (Novakouski & Lewis, 2012).

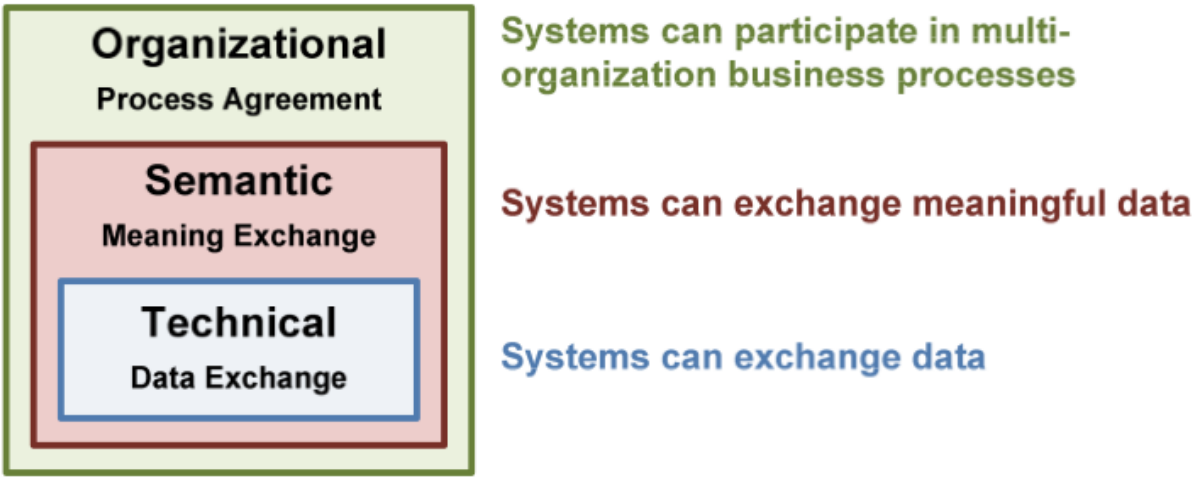

Figure 1 - Interoperability levels (Novakouski & Lewis, 2012, p. 9)

As we can see by the figure above (Figure 1) technical interoperability is placed at the base level, according to Novakouski and Lewis (2012) because data exchange is the root of all

communications. Semantic interoperability is placed above technical because in order to be able to exchange meaningful information one will have to be able to successfully exchange data. Organizational interoperability is placed at the top of this figure because one cannot have process agreement without the previous two levels (Novakouski & Lewis, 2012).

2.2 Risk Management

This section presents the concept of risk management, starting with definitions of risk, the different types of risk management and then a general overview of the risk management process.

2.2.1 What is risk?

The concept of "risk" has emerged over the past 30 years, but the word has been in the English language since the mid seventeenth century. The origin of the word is either from the Arabic word *risq* or the Latin word *riscum* (Merna & Al-Thani, 2008). The Arabic word risq means *"Anything that has been given to you [by God] and from which you draw profit"*. The Latin word *riscum* refers to the *"challenges that a barrier reef presents to a sailor"* (Merna & Al-Thani, 2008, p. 9). We can see that the Arabic version views risk as positive and will give a favorable outcome whereas the Latin word has a negative view and will give an unfavorable event. One thinks that the word "risk" entered the English language during the mid-seventeenth century, and it appeared in insurance transactions during the eighteenth century.

Since then the word has evolved and today we have many definitions. Risk is a concept that is challenging to define, understand and manage. This is because risk can mean different things to different people and/or organizations and there are many different definitions in use.

According to PMBOK (2008) and PMI (2009) risk is an *"uncertain event or condition that, if it occurs, has an effect on at least one project objective"*. PMBOK describes the objectives as scope, cost, quality and schedule. A fifth objective in risk management can be technical constraints (Conrow, 2000). Conrow (2000) defines risk as *"a measure of the potential inability to achieve overall program objectives"*. Both definitions contain two important components or dimensions: uncertainty and effect on objectives. The widely used ISO 31000 Standard for Risk Management also uses the word uncertainty in their definition; *"effect of uncertainty on objectives"* (R. J. Chapman, 2011, p. 334). As we can see "uncertainty" plays a role within Risk Management.

Uncertainty can be defined as an *"unpredictable event that disturbs operation and performance"* (Koh & Simpson, 2005). Lipshitz and Strauss (1997) did an extensive study on uncertainty and developed a list of 14 definitions. *"A situation in which one knows only the probability of which of several possible states of nature has occurred or will occur"* and *"The inability to assert with certainty one or more of the following: (a) act-event sequences; (b) event-event sequences; (c) value of consequences; (d) appropriate decision process; (e) future preferences and actions; (f) one's ability to affect future events"* are two of the definitions they use. Joseph (2010) defines uncertainty as *"a condition in which the decision maker does*

not know all the alternatives, the risk associated with each or the consequences each alternative is likely to have".

It is worth mentioning that risk and uncertainty are not the same. According to Alleman (2002) *"risk involves knowing the range of the outcomes; uncertainty involves not knowing the range of outcomes".* Also Remenyi (2012) supports this by writing that risks in a project are *"frequently known and can be managed"* and that uncertainties refer to a situation with *"little or even no knowledge of what the outcomes might be"*. Additionally risk implies that one can use probability to identify an expected outcome (Remenyi, 2012).

When talking about risk many see it as a downside, and something negative that can happen to your project or organization. Risks can be viewed with both an upside and/or a downside. One can say that upside risks are opportunities, while downside risks are threats (R. J. Chapman, 2011). Opportunity can be defined as *"a condition or situation favorable to the project, a positive set of circumstances, a positive set of event, a risk that will have a positive impact on project objectives or a possibility for positive changes".* In contrast with a threat, which can be defined as *"a condition or situation unfavorable to the project, a negative set of circumstances, a negative set of events, a risk that will have a negative impact on a project objective if it occurs, or a possibility for negative changes"* (PMI, 2009).

According to C. Chapman and Ward (2007) *"All projects involve risk—the zero risk project is not worth pursuing. This is not purely intuitive but also a recognition that acceptance of some risk is likely to yield a more desirable and appropriate level of benefit in return for the resources committed to the venture. Risk involves both threat and opportunity".*

Risk, uncertainty, or failing to achieve an outcome, can be described using the term probability or likelihood. The Project Management Institute (2009) defines probability as *"a measure of how likely an individual risk is to occur".* The effect may be described as the impact or consequence of failing to achieve the specified outcome (Conrow, 2000; PMBOK, 2008). The effect can be negative or positive on the objectives (Hulett, 2004).

Risk can be calculated using a formula or equation using probability, likelihood severity, impact, and so on. Cioaca (2011) uses two other formulas in her article, namely *Risk = probability × impact* and *risk = frequency x severity.* Bahill and Smith (2009) did a research of all equations used in published literature and the following eight are the result:

- Risk = Severity of Consequences × Frequency of Occurrence
- Risk = Severity of Consequences × Likelihood of Occurrence
- Risk = Severity of Consequences × Estimated Probability
- Risk = (Impact + Likelihood)/2
- Risk = Severity + Probability - (Severity × Probability)
- Risk = Severity × Probability × Difficulty of Detection
- Risk = Severity^2 × Probability
- Risk = Severity × Exposure

Bahill and Smith (2009) use the top two in their article and we can see that these two match the formula used by Cioaca (2011).

2.2.2 What is Risk Management?

Risk Management has taken center stage and a review of the history shows that the risk management practice *"has been inadequate"* (R. J. Chapman, 2011, p. 3). We find risks in all projects and that is why risk management has become an important part of project management. According to Merna and Al-Thani (2008) one can say that the aim of risk management is to *"identify risks specific to an organization and to respond to them in an appropriate way"*. Risk Management is a formal, continuous process throughout the entire life cycle of a project (Merna & Al-Thani, 2008; Northrop Grumman Coroporation, 2007). The Risk Management approach and process will be discussed later in chapter 2,3. Just as risk has many different definitions so has risk management. Merna and Al-Thani (2008) use the following definition: *"Risk management is a formal process that enables the identification, assessment, planning and management of risks"*. Other authors define risk management as *"the entire process of actively considering risks in project context"* (Powell & Klein, 1996).

Further Powell and Klein (1996) state that the purpose of risk management is to *"select a course of action which provides an acceptable balance between likely benefits and exposure to risk"*. According to Kutsch (2008) the purpose of risk management is to *"manage risk in advance […] to respond to risks that may have a future adverse impact on the project outcome"*. A risk management strategy is necessary to survive in today´s market place (Merna & Al-Thani, 2008). With today´s pace people are *"less likely to recognizing the unusual"* and the pace of change makes it difficult to detect risks. This is because the organizations and other variables are constantly changing. Introducing project risk management early will give a better chance of dealing with risks (Hulett, 2012).

There are many different categories of risk management. According to R. J. Chapman (2011) businesses faces six different classes of risk exposure.

Financial Risk Management is about the financial risk your business can encounter. Financial risk is *"the exposure to adverse events that erode profitability and in extreme circumstances bring about business collapse"* (R. J. Chapman, 2011).

Operational Risk Management relates to business risk, disaster risk, legal risk, system risk, regulatory risk and outsourcing. Operational risk is *"the risk of loss resulting from inadequate or failed internal processes, people and system or from external events"* (R. J. Chapman, 2011).

Technological Risk Management is related to the internal processes in regards of technology. Technological Risk is defined by R. J. Chapman (2011) as *"events that would lead to insufficient, inappropriate or mismanagement of investment in technology"*.

Environmental Risk Management is related to related to the environment and energy. According to R. J. Chapman (2011) *"environmental risk is the deterioration of bottom-line performance from increased regulation of energy usage, eroded reputation from an*

environmental incident, increased costs form the effects of global warming" and so on. This can also be related to loss of oil production, pollution or severe weather conditions.

Enterprise Risk Management relates to managing risk in the entire enterprise. It is a response to the use of the silo-based approach of managing risks independently. Enterprise risk management (ERM) is used to improve performance in the overall business and to gain a deeper understanding of the interdependencies between risks. ERM is defined as *"a comprehensive and integrated framework for managing company-wide risk in order to maximize a company's value"* (R. J. Chapman, 2011).

Project Risk management can be defined as the process of *"conducting risk management planning, identification, analysis, response planning, and monitoring and control on a project"* (PMBOK, 2008). Risk Management is simply the act of dealing with risks. To achieve this one should *"increase the probability and impact of positive events, and decrease the probability and impact of negative events"* (PMBOK, 2008).

My focus in this study has primarily been on Project Risk Management related to IT projects.

2.2.3 Risk Management in the public sector

As mentioned in the introduction there has been an increase in the focus of risk management in the public sector in both UK and US (Duggan, 2006; Hofmann, 2008). More and more organizations focus on risks and according to both Duggan (2006) and Hofmann (2008) the public sector faces a challenge when it comes to risk management.

Risks can be found in many areas within the public sector and e-governance, because the projects have a wide scope and are complex. *"E-Governance projects are unique undertakings that involve degree of uncertainty and inherently risky"* (Choudhari et al., 2006). According to the same authors a challenge within eGovernment is that risk management and e-governance projects are *full of risk and uncertainties"* (Choudhari et al., 2005). Research focuses on risk factors, but there is little attention to risk assessment frameworks and e-governance in the literature (Choudhari et al., 2006).

According to Tiatasin (2012) risks within e-governance can be found in five areas; IT Infrastructure risk, Economic risk, Legal and regulation risks, Change Management Risk and Performance Risk. Choudhari et al. (2006) writes about identifying risk as important and mentions one method called a checklist. A checklist can be used to identify certain risks and focus on *"subset known and predictable risk"* (Choudhari et al., 2006).

Another important aspect of risk within e-governance is trust and security. Citizens want to be sure that their online interaction is secure and if they don't find the services to be secure and trustworthy the citizens will most likely not use them (Bélanger & Carter, 2008). According to Bélanger and Carter (2008) *"trust is an essential element […] when uncertainty, or risk, is present"*. The majority of Americans distrust the government. The U.S Citizens prefer security and privacy over an expansion of the benefits offerings from eGovernment through online services. This is closely related to the citizens use and acceptance of new technology

(Whitmore & Choi, 2010). Whitmore and Choi (2010) point to that *"U.S. citizens prefer a slower pace of expansion"*.

In order to succeed with e-governance and reduce the risks one need to communicate with the citizens. Whitmore and Choi (2010) mention seven cardinal rules of risk communication:

1. Accept and involve the public as a legitimate partner
2. Plan carefully and evaluate your efforts
3. Listen to the public´s specific concerns
4. Be honest, frank, and open
5. Coordinate and collaborate with other credible sources
6. Meet the needs of the media
7. Speak clearly and with compassion

Hwang, Li, Shen, and Chu (2004) suggest eight classifications of communication in e-governance, where one can communicate between and across Government, Officeholder, Citizen and Business. Zhou and Hu (2008) point to three types of communication; communication inside government, between different governments and between the government and society. With the variety of ways to communicate we can see that this can be a challenge, and that there is a need to manage it properly.

Wibowo and Yuwono (2008) provide a list of enablers for IT governance and awareness of risk management is ranks high. Risk awareness is in some cases related to having a risk committee. The authors also point to the importance of understanding and having this awareness combined with understanding will be a good basis of good leadership from the top management. Performing risk assessment during the whole project life cycle is also deemed as important.

Braig et al. (2011) created a list of seven barriers to risk management and five recommendations to strengthening risk management in the public sector. Leaders who lack knowledge of risk management, limited risk culture and mind-set, and lack of clear risk metrics are some of the barriers. The recommendations they propose are:

1. Create transparency both internally and externally
2. Develop a "risk constitution"
3. Initially focus in modifying a few core processes
4. Establish a dedicated risk-management organization
5. Build a risk culture

Risk culture is closely related to risk awareness and according to Hopkin (2012) it is vitally important. The organization can achieve a risk aware culture when team members and top management "*understand and accept the importance of adequate risk management"*. Good communication and sharing of information is required to have a risk-aware culture and sharing risks throughout the organization will enhance the risk awareness (Hopkin, 2012).

Risks and issues with interoperability become more difficult when two or more organizations are collaborating. Potential challenges with interoperability can be if the collaborating

organizations have different risk management cultures or different goals. An issue that arises here relates to *who* should have the main responsibility of risk management (Adams, Waldherr, & Lee, 2007). Interoperability has become increasingly significant in the EU in recent years and it is mentioned as an essential prerequisite for e-governance (Misuraca et al., 2011).

2.2.4 IT Risk

Risk is something that always will be present. IT Project Risk management is a topic that has been researched for more than 30 years, and is still a challenge for many organizations. There is a common interest in the area of risk and uncertainties in IT projects, and we can see this by the number of researchers (Boehm, 1991; Chulkov & Desai, 2005; Schneider, Lane, & Burton, 2009; Taylor, Artman, & Woelfer, 2012). Despite these 30 years of research, one can see that there are still IT/IS projects failing (Bakker et al., 2009; Chulkov & Desai, 2005; Kappelman et al., 2006; Powell & Klein, 1996; The Standish Group, 1994, 2009). There are several examples of IT projects failing and some examples are the London Ambulance System in the UK, FoxMeyer in the US (Remenyi, 2012) and Tress90 in Norway. Although there is a consensus on IT a project failure, there is no agreement on the percentage of IT project failures.

The Standish Group (1994) published a much criticized and cited report called the CHAOS report in 1994. In this report we can read that the success rate of IT projects is as low as 16,2%, giving us a failure rate of 83,8%. The same company published a new comprehensive report in 2009 called the CHAOS summary (The Standish Group, 2009). In this report we can read that the success rate has gone up to 32%, leaving us with a failure rate of 68%. Remenyi (2012) writes in his book, Stop IT project failures through risk management, about different authors who points to failure rates between 15% and 85%.

The reason for this high failure is that managers and businesses do not manage the risks (McNurlin & Sprague, 2009, p. 367). There are many authors who write about reasons for IT projects failures. Neimat (2005) points to poor planning, unclear goals and objectives, lack of executive support, and failure to communicate and act as a team.

Poor planning relates to not spending enough time planning during the startup phase of the project. Included in this phase is risk calculation, which also will be conducted poorly. *"Not doing an explicit risk calculation is one of the major problems with project planning"* (Neimat, 2005). Unclear goals and objectives relate to the poor gathering of relevant information in the definition phase of a project. Defining requirements is a time-consuming activity and requires good communication, but is sometimes not well conducted due to difficulties on describing what the goal of the project is. Lack of executive support is a factor that can have a big impact on the project. It relates to the executive management to be open about what they think and believe about the project. Executive management support is also important in order to make the right priorities in a project. Failure to communicate is something that Neimat (2005) points out as being a common problem on IT projects.

Kappelman et al. (2006) did extensive research on reasons for IT project failure and early warning signs and came up with a list of no less than 53 ranked reasons for failure. Lack of top management support, requirements and scope is not documented, lack of effective communications and weak project management are only a few of the reasons they listed.

Lack of top management support did not come as a surprise to the authors as being ranked as the number 1 reason for IT projects failure. The reason for this is that employees tend to do what the management think is important. This factor is closely related to "weak project management". Mangers who lack the skills of effective managing and communication are a risk for IT projects. Effective communication is important among management, stakeholders and employees or else the employees will be pulled in multiple directions. Kappelman et al. (2006) also write that one needs risk management to be able to avoid risk.

According to Powell and Klein (1996) the reasons for failure in IS projects are seldom related to risk in projects and an approach to manage such risk are seldom considered. Furthermore, more recent studies (e.g. Schneider et al. (2009)) also suggest that the main reason for IT project failures is *"inadequate risk management"*. The IT industry is also known to be a fast growing industry with rapidly changes. The author also writes that IT projects are more likely to fail than other projects and that the cause of this failure is because the use of rapid changing technologies (Schneider et al., 2009). To survive today´s market and to maintain a competitive edge, one should develop and adopt IT (Merna & Al-Thani, 2008).

McCubbrey (2010) points to the IT risks being known to IT professionals, but not shared with others as a common problem. In the article the author has also listed some of the reasons why IT projects fail. They are inadequate understanding, poor planning, identification and estimation, failure to address problems and no fallback plan (McCubbrey, 2010). Bakker et al. (2009) did an extensive research on IT project risk and found that the knowledge of risk is not enough to make a project successful. Further the authors show that managers ignore risk, avoid risk, or delay their actions pending improvement in the circumstances (Bakker et al., 2009).

New technology is a challenge, which can be the reason for the high degree of project risk (Chulkov & Desai, 2005). Other factors and categories, which can explain the high degree of risk in IT projects are project management risk, relationship risk, solution ambiguity risk and environment risk (Taylor et al., 2012). Also Powell and Klein (1996) point to the need for project management to address risks.

Several authors point to risk factors related to IT or IS. Sumner (2000) points to changing scope, lack of technical expertise, lack of application knowledge, lack of adequate technology infrastructure and lack of measurement system for controlling risk as some of the risk factors related to implementation of IT. Both Sumner (2000) and Boehm (1991) point to misunderstanding requirements and changes in requirements and poor communication as being risk factors for IT projects. Tesch, Kloppenborg, and Frolick (2007) collected 92 risk factors from several other authors. The 92 risk factors were then divided into groups; sponsorship/ ownership, funding and scheduling risks, personnel and staffing, scope, requirements and relationship management. Some of the risk factors are; introduction of new

technology, lack of a documented project plan, poor project management, inadequate top management commitment and lack of enough staff or those with the right skills.

A survey from 2010 listing the top challenges for risk management shows that the number one challenge for companies is lack of risk management dedicated staff and personnel (Hofmann, 2010).

Based on this we can see that IT/IS risk management is challenging and this needs to be addressed. *"The effect of risk and uncertainties can be very significant"* (Intaver, 2004). Further, the author writes that projects with risks should be proper analyzed at the planning stage of the project and then reassess the risks during the project's life cycle. Every project should have a risk management plan and risk analysis is one of the most important steps of this process (Rot, 2008).

2.2.5 Critical success factors for risk management

To be able to successfully manage the risks in a project there are some key factors to consider. Some authors have written about key success factors and critical success factors for risk management. According to Hillson and Simon (2007) the *"common reasons for not applying risk management can be overcome by focusing on critical success factors"*. The authors have grouped the CSF´s into four categories: Supportive organizations, competent people, simple, scalable process and appropriate methods, tools and techniques.

Hulett (2004) describes why businesses and organizations do not do risk management; they do not understand how risk contributes to results. Hopkinson, Close, Hillson, and Ward (2008) write that a *"clear understanding of risks is essential"*. Also Intaver (2004) describes that managers and businesses do not believe in risk management being beneficial. Several authors points to the importance of doing *something* with their risks, and that they should pay special attention to risk management (Bakker et al., 2009; Cioaca, 2011; Letens, Nuffel, Heene, & Leysen, 2008).

Grabowski and Roberts (1999) researched the problem with risk mitigation. They identified four important factors for good risk mitigation:

1. Organizational structure and design
2. Communication
3. Organizational culture
4. Trust

Faisal, Banwet, and Dhankar (2006) also researched risk mitigation and identified a long list of enablers. Some of the enablers in the study are information sharing, Risk sharing and Knowledge. Information Sharing relates to communicate and coordinate effective and by doing so one can reduce the risks. Faisal et al. (2006) point to information sharing as a *"prerequisite for trust"*. The final factor of information sharing is that it can *"minimize the consequence of the bullwhip effect"* (Faisal et al., 2006).

Risk sharing relates to sharing risks both with the project team but also other involved, e.g. stakeholders or other suppliers. Knowledge about risk is an enabler related to understanding and that improved understanding can help make better decisions and decrease the risks (Faisal et al., 2006).

Williams (2004) presents a list of six key factors for successful risk management. The factors are be proactive, systematically surface risks, all stakeholders must communicate, prioritize risks, develop a "top 10" risk list and utilize a risk-driven process.

Harner (2010) have written an essay about barriers to effective risk management and some of the barriers mentioned are lack of integration and communication. She writes that both these barriers appear to be one of the most significant. Another barrier mentioned in her paper is the need for better understanding regarding risks.

Kutsch (2008) studied barriers to project risk management related to IT projects and found five categories through his literature review. The top barrier for optimal and effective project risk management is according to Kutsch (2008) lack of hindsight. This relates to the project manager not relying on the validity of probabilistic conclusion about future risk based on historical date. The other problems identified by Kutsch (2008) are problem with ownership, problems with cost justifications, lack of expertise, lack of arousal and problem of ambiguity in risk estimates (Kutsch, 2008). Problems with ownership relate to that the risk owners do not feel responsible because *"they are perceived to be owned by someone else"* (Kutsch, 2008). According to R. J. Chapman (2011) risk management is most effective when *"ownership of risk is allocated to an appropriate senior official"*.

2.3 Good practice for risk management

As mentioned, Risk Management is a continuous process rather than a linear and static process. All organizations face risks and need to manage them in some way. Risk management has been conducted in many years and it is increasingly applied. The process of risk management is described in a variety of risk management standards or frameworks.

The purpose of having a risk management standard or framework is to help the organization make risk management an integrated part of the management processes so that risk management can become a regular activity. The aim of having a framework is to ensure that information about risks is processed and reported adequately and that this information is used as a basis for decision-making (R. J. Chapman, 2011).

The four most common phases of a risk management process are risk identification, assessment, response planning and monitoring. Typically the risk management process consists a variation of these processes (Taylor et al., 2012). Kutsch (2008) argues that best practice project risk management processes can be deconstructed into four stages; planning, identification analysis and responds. These four phases are not similar to the ones presented by Taylor et al. (2012), but we can see that the processes are similar only labeled differently.

2.3.1 General risk management approach

As mentioned above, the four most common phases in a risk management process is risk identification, assessment, response planning and monitoring. In total seven possible steps were identified through a comparison of different standards, national and international. All steps are described below with examples of tools and techniques that can be used. Thereafter the comparison is presented in chapter 2.3.2.

Identify risks involves finding the risks that may affect the project and document the findings. The process is iterative and should always be looked at. This is because new risk may evolve and occur and these should be documented. The frequency of risk identification will vary for each project. In this process one should have as many participants as possible. PMI suggest the following: *"project manager, project team members, risk management team, customers, subject matter experts from outside the project team, end users, other project managers, stakeholders and risk management experts*" (PMI, 2009).

For the identification phase, the use of checklist and brainstorming are widely used. A checklist can be viewed as a historical review and is based on previously projects. Brainstorming is viewed as a creative activity where all stakeholders can be involved.

Risk analysis can be done either qualitative or quantitative. The process of performing qualitative risk analysis includes looking at every individual risk and prioritizes them. It also includes evaluating the probability and the effect of each risk. In the qualitative risk analysis one should also categorize the risks according to source or cause. This type of analysis should always be performed within a project (PMI, 2009).

Quantitative analysis includes analyzing the effect the identified risks may have on the overall project. This is done in a numerical process. The output of this process will be an estimate based on the project plan and other information that are currently available. This type of analysis is not as required as the qualitative, but one should perform it to get an overview on the project (PMI, 2009).

For the analysis phase we have two different sets of tools, one for the qualitative analysis and another for the quantitative analysis. For performing qualitative risk analysis we can use estimation techniques or Probability and Impact Matrix. Estimation techniques relates to looking at both probability and impact. The Probability and Impact Matrix allows organizations to prioritize the risks either for further analysis or for risk response (PMI, 2009). A Probability and Impact Matrix is also called risk matrix and is often used to *"segregate high-impact risks from low-impact risks"*(Merna & Al-Thani, 2008). A risk matrix can be made in a 3x3, 4x4 or 5x5 table, using the colors green, yellow and red as seen by the figure below (Figure 11). The figure is an example of a 3x3 risk matrix.

Figure 2 - Risk matrix

The risks placed in the top right corner are considered to be critical risks and the risks placed on yellow can be threatening. Risks placed in the bottom left corner are green and considered to be ok. The colors also represent the severity of the risk, where green is low severity and red is high severity (R. J. Chapman, 2011). As mentioned earlier, risk can be calculated using probability and consequence, and later put into a risk matrix.

For performing quantitative risk analysis we have other tools and techniques. Monte Carlo simulation and Decision Tree Analysis are two of the techniques. The most known and accepted tool for analyzing uncertainty is called Monte Carlo Simulation and it is primarily used for project schedules and gives an answer of how likely it is to be successful and how much contingencies one needs to achieve the goals.

Prioritize risk relates to determining what risks to take actions on and/or mitigate first. This step is usually included in the analysis phase, but some choose to have it as a separate phase.

Risk Response is the step after Analysis. The purpose of this step is to determine responses to the individual risks and the project risks. Determining responses means setting actions to the risk and finding the actions witch gives the higher probability of success. When the risks have been identified and analyzed one should develop a plan that addresses all the risks. The risk responses should be included and described properly with trigger conditions. There are four approaches on how to respond to risks: Avoiding, reducing, sharing and accepting (PMI, 2009).

Techniques for risk response can be contingency planning, multi-creation selection techniques or scenario analysis. A scenario analysis relates to creating several plausible alternative

scenarios, and then the organization can choose between the different scenarios. Different scenarios may require different risk responses.

Monitor and control The main purpose of this step is to monitor and control the identified risks, identify new risks, ensure that the risk responses are being executed at an appropriate time, monitor residual risks and evaluate the entire risk management process. The benefit of performing this is to continuously improve and optimize the process throughout the project life cycle (PMI, 2009).

For monitoring and controlling risks one can use risk audits, status meetings, risk reassessment or trend analysis.

2.3.2 Comparison of the different frameworks

Some of the standards that exist are listed below. They will be further explained later in this section.

- Australian Standard/New Zealand Standard (AS/NZS 4360) – Risk management – Principles and guidelines
- The institute for Risk Management, ALARM The National forum for Risk Management in the Public Sector, The Association of Insurance and Risk Managers (IRM, ALARM, AIRMIC) – A Risk Management Standard
- Information Systems Audit and Control Association (ISACA) – The Risk IT Framework
- International Organization for Standardization (ISO) 27001 - Information technology - Security techniques - Information security management systems - Requirements
- International Organization for Standardization (ISO) 27005 - Information technology - Security techniques - Information security risk management
- International Organization for Standardization (ISO) 31000 - Risk management - Principles and guidelines
- Norwegian Standard (NS 5814) – Requirements for Risk Assessment
- Project Management Institute (PMI) – Practice Standard for Project Risk Management

In addition to the standards and framework listed above, there are a variety of corporate frameworks in Norway and some of them are listed below (freely translated):

- COSO/NIRF (Committee of Sponsoring Organizations of the Treadway Commission/The Institute of Internal Auditors Norway) – Enterprise Risk Management – Integrated framework
- The Norwegian Government Agency for Financial Management (DFØ) – Risk Management in the government – Managing risks in objective and performance management
- The Agency for Public Management and eGovernment (DIFI) – Risk Assessment – a guide to the Framework for authentication and non-repudiation of electronic communication in the public sector

- The Norwegian Data Protection Authority (Datatilsynet) – Risk assessment of information system
- The Norwegian Directorate of Health (Helsedirektoratet) – Norm for Information Security

As we can se by the two lists presented, there are many standards for Risk Management and the table below (Table 1) gives an overview of the processes for each standard. After the table is presented a small description of each standard will be given. At the end a summary is presented.

	Plan	Identify	Analyze	Prioritize	Estimate and assess	Response	Monitor and Control
AS/NZS 4360	X	X	X		X	X	X
COSO/NIRF		X			X	X	X
DFØ	X	X			X	X	X
DIFI		X	X	X	X	X	
IRM, ALARM, AIRMIC		X	X		X	X	X
ISACA		X	X			X	X
ISO 27001	X	X	X		X	X	X
ISO 27005	X	X	X		X	X	X
ISO 31000	X	X	X		X	X	X
NS 5814	X	X	X		X	X	
PMI	X	X	X			X	X
The Norwegian Data Protection Authority	X	X			X	X	
The Norwegian Directorate of Health	X	X			X		

Table 1 - Comparison of different frameworks

Australian /New Zealand Standard (Australian/New Zealand Standard, 2009) was developed by the Joint Australian and New Zealand committee. The standard provide a generic guide to risk management and is applicable in a variety of organizations and activities, public, private and community. In 2005 the International Organization for Standardization (ISO) developed the first international risk management standard and they used the AS/NZS 4360 as basis. The figure below (Figure 2) gives an overview of the Australian/New Zealand standards process:

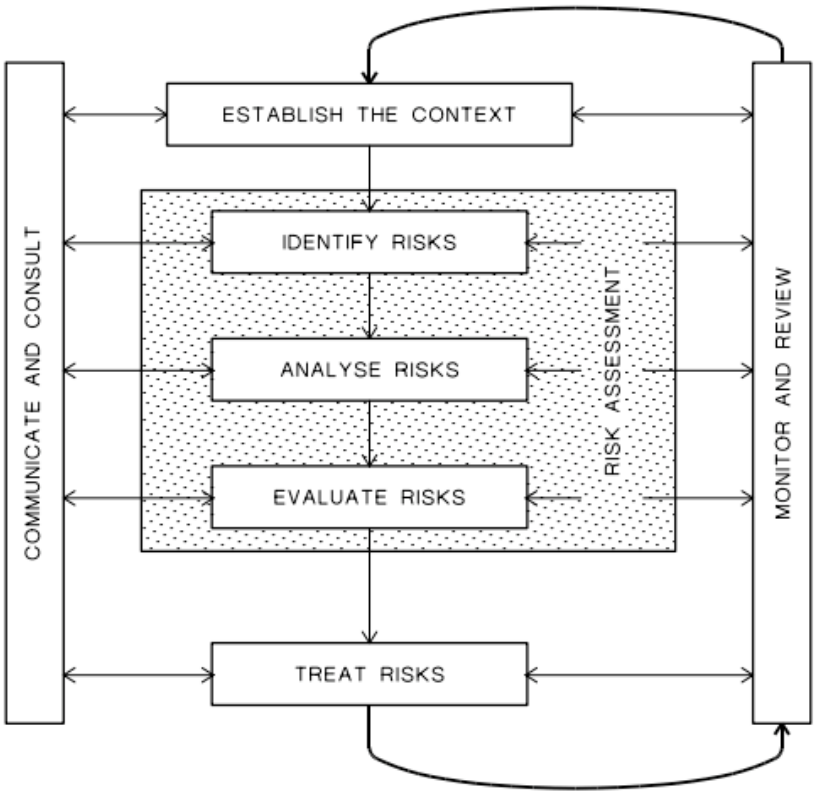

Figure 3 - AS/NZS ISO 31000:2009 – Risk management – Principles and guidelines (Australian/New Zealand Standard, 2009, p. VI)

The NIRF framework, Enterprise Risk Management – Integrated Framework (NIRF, 2005) is identical to the COSO framework. What distinguishes them is that NIRF is a Norwegian translated version of the original COSO framework. This is a framework for the entire enterprise, and is called enterprise risk management. The process is not serial, but multidirectional and iterative where any component can influence the others. The figure below (Figure 3) gives an overview of the process:

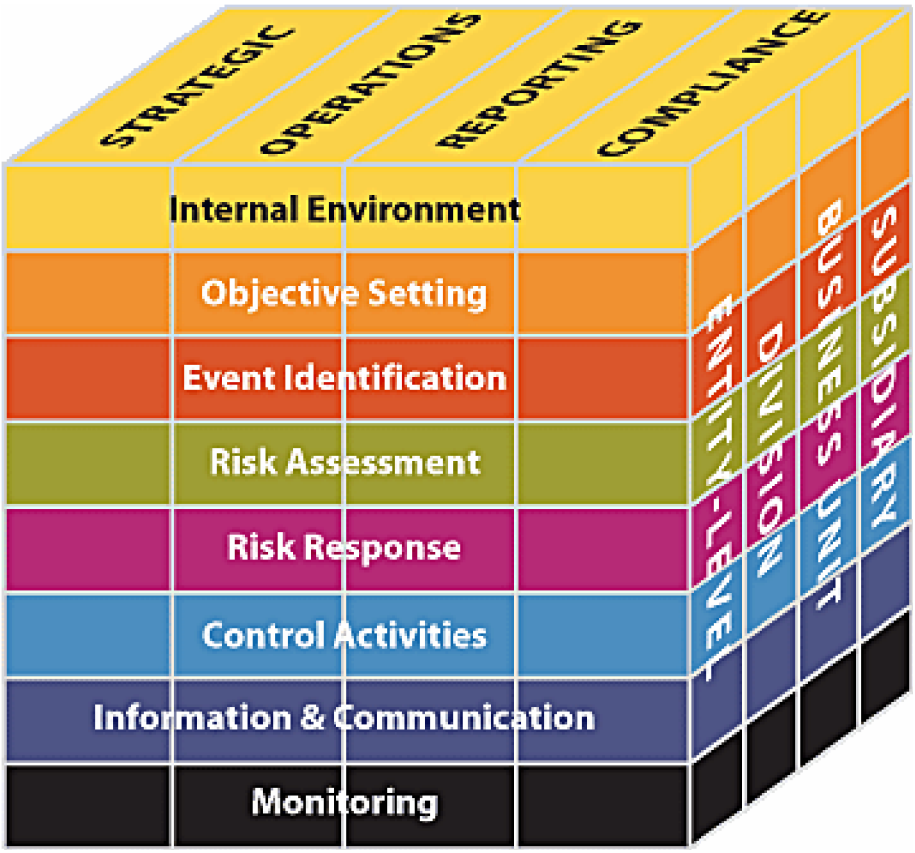

Figure 4 – Enterprise Risk Management – Integrated framework (NIRF, 2005, p. 4)

DFØs' framework, Risk Management in the government – Managing risks in objectives and performance management (DFØ, 2005), is a Norwegian framework aimed at the public sector. It is based on the recognized international framework, COSO, which is explained above, and tailored for government financial regulations and state requirements. The figure below (Figure 4) is freely translated and gives an overview of the process:

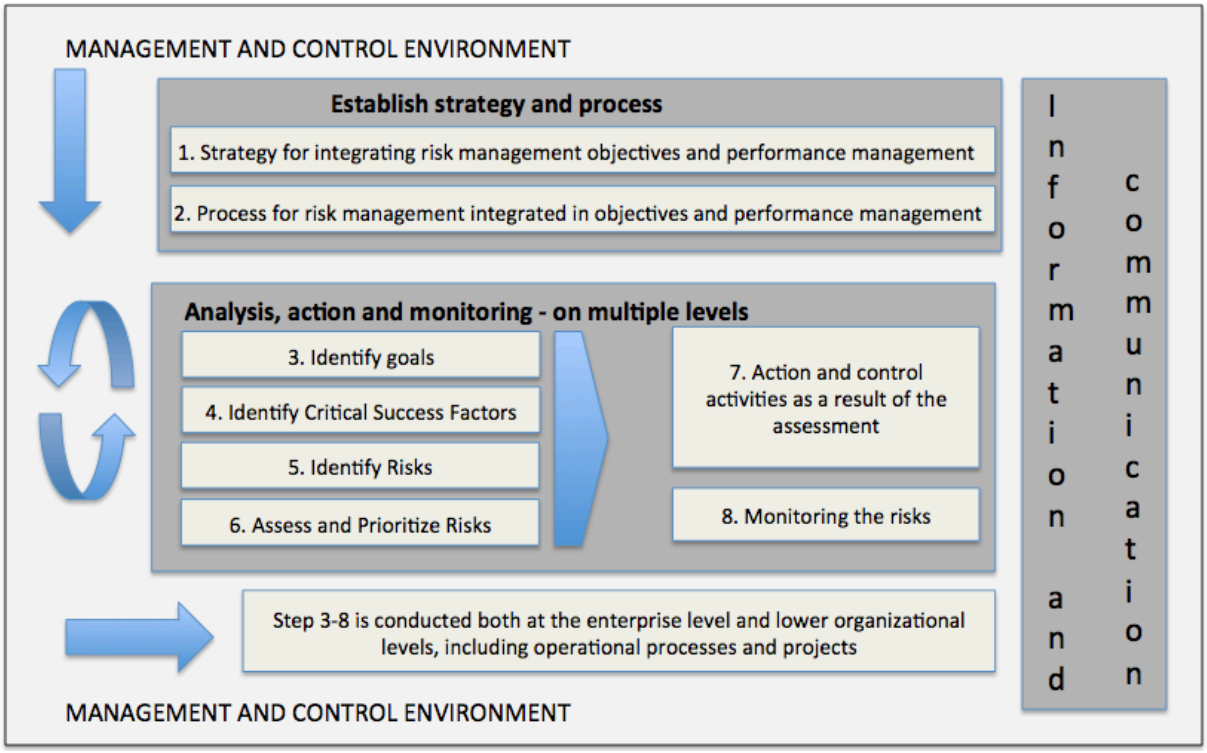

Figure 5 - Risk Management in the government – Managing risks in objectives and performance management (DFØ, 2005, p. 8)

DIFIs framework, Risk Assessment – a guide to the Framework for authentication and non-repudiation of electronic communication in the public sector (DIFI, 2010), is also guided towards information security and confidentiality, integrity and availability. It is based on ISO 27001, 27005 and 31000, The Norwegian Data Protection Authority and others. The structure they propose consist of six steps; Plan, identify, analyze, assess, prioritize and response. An overview of the process can be seen in the figure below (Figure 5). The figure is freely translated.

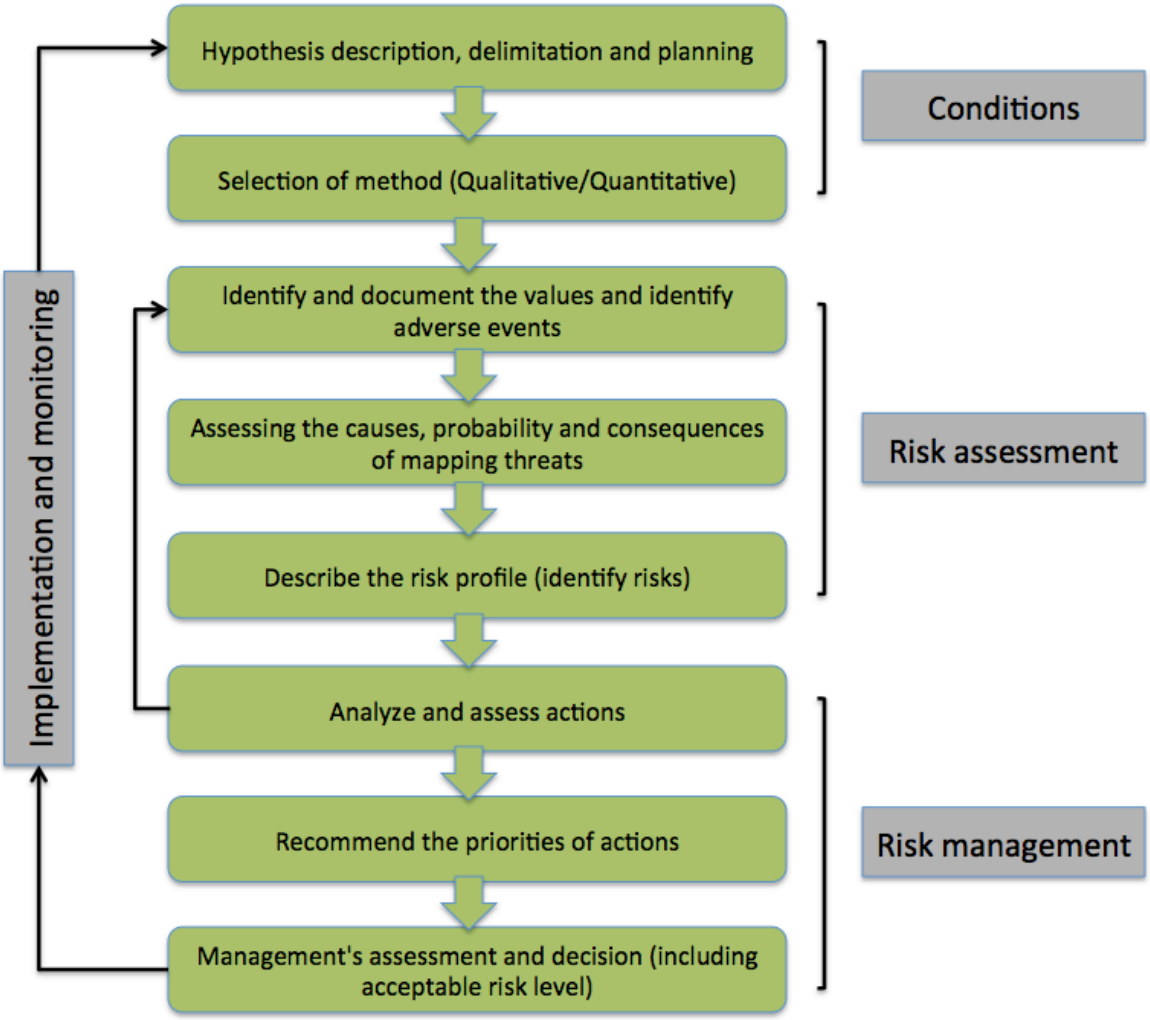

Figure 6 - Risk Assessment – a guide to the Framework for authentication and non-repudiation of electronic communication in the public sector (DIFI, 2010, p. 8)

IRM, ALARM AIRMIC's standard, A Risk Management Standard (AIRMIC, ALARM, & IRM, 2002), is a standard written by three major risk organizations in the UK and it represents best practices. The standard is based on terminology from ISO wherever that was possible and it is therefore similar to the ISO standards (ISO 27001, 27005 and 31000). The structure they propose can be view in the figure below (Figure 6):

Figure 7 – A Risk Management Standard (AIRMIC et al., 2002, p. 4)

ISACAs framework called RiskIT (ISACA, 2009) is guided towards IT risk and IT governance. It is based on Enterprise Risk Management Standards such as COSO and ISO 31000. It is a framework for the entire enterprise for successful IT risk management. It is *"based on a set of guiding principles for effective management of IT risk"*. The figure below (Figure 7) gives an overview of the RiskIT framework:

Figure 8 – The RiskIT Framework (ISACA, 2009, p. 15)

The ISO Standards are very similar to each other and are based on each other. Both ISO 27001 and ISO 27005 relate to Information technology, Security techniques, and Information Security Management Systems. ISO 27001 is the standard recommended by DIFI (DIFI, 2012) for the Norwegian government. ISO 27001 relates to requirements and 27005 relates to the framework. The process of these two is based on ISO 31000. ISO 3100 was the first international standard for risk management and it was adopted and based on the Australian and New Zealand Standard 4360. ISO 31000 is a general risk management standard. All three ISO standards mentioned are also based on a generic loop of "Plan – Do – Check – Act". The process proposed in these ISO standards is iterative and consists of 7 steps; Establish, Identify, Analyze, Evaluate, Treat, communicate and consult, and monitor and review. As seen by the figure below (Figure 8) Communicate and consult, and monitor and review are continuous processes.

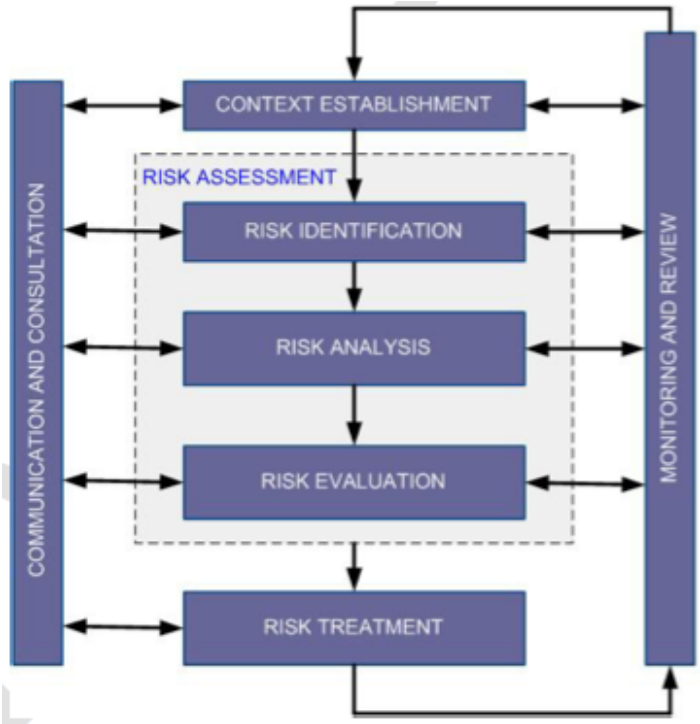

Figure 9 – ISO 27001, ISO 27005 and ISO 31000 framework (ISO/IEC 27001:2005, ISO/IEC 27005:2008, ISO/IEC 31000:2009)

The Norwegian Standard – 5814, Requirements for Risk Assessment (Norsk Standard, 2008) is a general standard developed and primarily aimed at subjects, sectors and industries that do not have their own standard. Standards Norway is responsible for standardization tasks in Norway and has the sole right to determine and publish the Norwegian Standard. If one area lacks a standard, Standard Norway will develop one. They are also the Norwegian member of ISO. The Requirements for Risk Assessment Standard is aimed at risk assessment. Risk assessment in this case means planning and implementation of risk analysis and risk evaluation, as can be seen by the figure below (Figure 9):

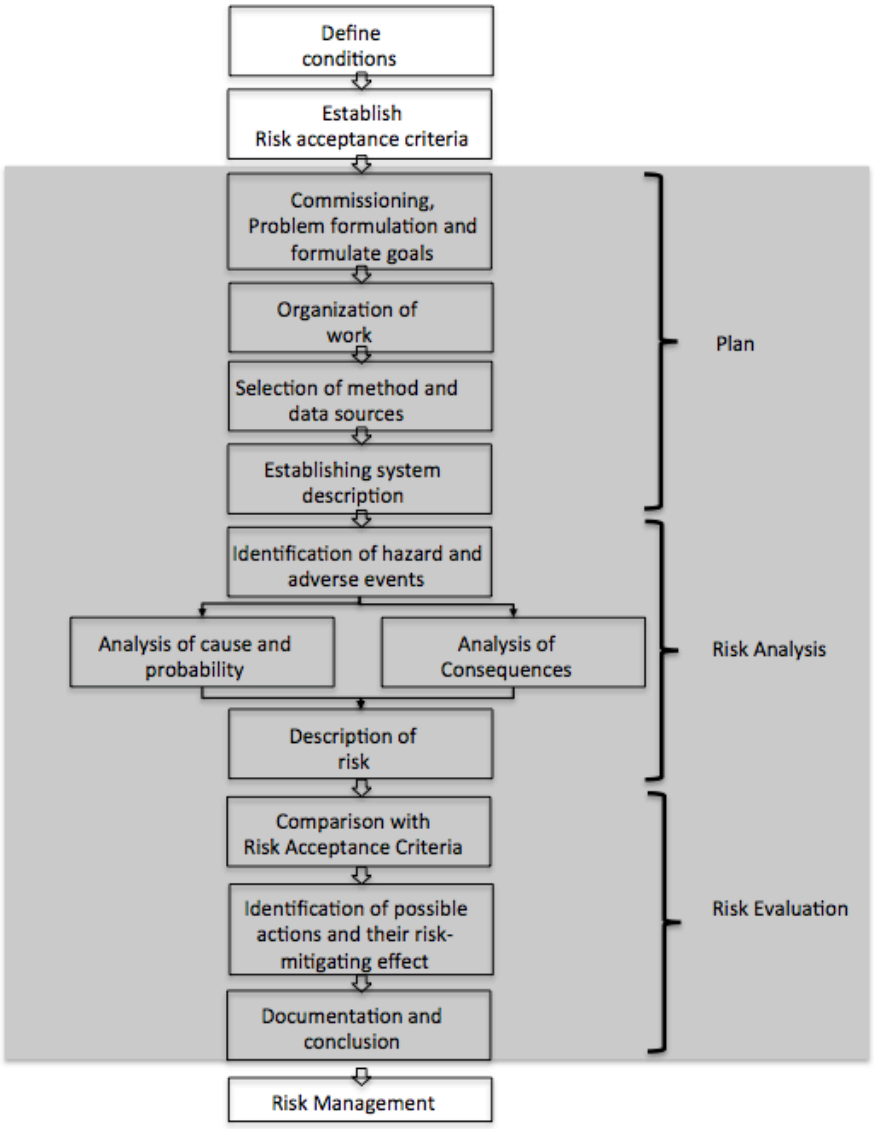

Figure 10 – NS 5814 - Requirements for Risk Assessment (Norsk Standard, 2008, p. 4)

Project Management Institutes framework, Practice Standard for Project Risk Management (PMI, 2009) presents tools and techniques for all steps. The framework is iterative and consist of 6 steps; Plan, identify, qualitative analysis, quantitative analysis, response and monitor and control. Some of the tools and techniques are brainstorming, SWOT, Risk Breakdown Structure and Checklists. The figure below (Figure 10) gives an overview of PMI's framework.

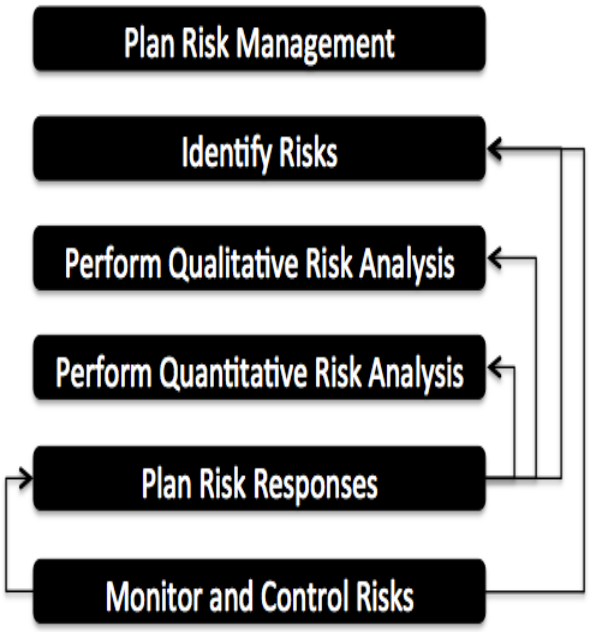

Figure 11 – Practice Standard for Project Risk Management (PMI, 2009)

The Norwegian Data Protection Authority (Datatilsynet) has a risk management framework for information security and is used in relations to confidentiality, integrity and availability. The method describes a structure to the risk management process consistent of four steps; Plan, identify and response. They propose using a risk matrix with probability X consequence in a 4x4 matrix.

The Norwegian Directorate of Health (Helsedirektoratet) also has a framework for information security. This is used for managing personal and health information, and confidentiality, integrity and availability. The framework was developed as collaboration between several organizations. The Norwegian Data Protection Authority, DIFI and The Norwegian Health Network are amongst those organizations. Organizations that work with personal information can use this. Risk should be assessed before starting working on personal information. They propose using a structured method consistent of five steps; plan, assess, identify, assess and response. In addition they propose using a risk matrix with probability x consequence.

2.3.2.1 Relationship between the international and the Norwegian standards

As we can see by the above comparison of different standards and frameworks, they are all corresponding with similarities in the proposed processes. The Australian and New Zealand framework and the ISO standards are similar and since the IRM, ALARM AIRMIC framework is based on ISO this framework has similarities to ISO. Since the NIRF framework is a translated version of COSO it is natural that those are similar, and than DFØ's is similar to those. The Norwegian Standard and DIFI are similar to the above-mentioned standards.

In December 2013 DIFI presented a report called *"Management system for information Security – Experiences and Recommendations of ISO 27001 and ISO 27002"* (DIFI, 2012). The report addresses experiences and recommendations on introducing of management systems for information security and assess if ISO 27001 and ISO 27002 should be made mandatory in the government and the public sector. As a base for the report they conducted an interview-based survey about the implementation and use of a management system for information security, with special emphasis on experience with ISO 27001. A finding presented in this report relates to the use of frameworks and methods. DIFI points out that finding appropriate methodology and templates for risk assessment seems to be a major challenge. One of DIFIs interviews stated *"We are a bit confused here when DFØ, DIFI and The Norwegian Data Protection Authority publishes different guidelines in the same topic. What should we use?"* (DIFI, 2012).

2.4 Summary of literature

In the literature review risk and risk management in relation to interoperability and the barriers that can occur have been examined. In this section a short summary of the literature is presented and an answer to the first two research questions are presented.

There has been a shift in they way the public sector works and there are several examples of this in Norway. The Norwegian Government have published a program related to a digitized government and The Norwegian Tax Administration have made health care services available online and digitized. The Agency for Public Management and eGovernment (DIFI) have developed an online *"project wizard",* which aims at helping to improve the ability to implement digitization projects and improve the success rate of such projects.

We have seen that risk management has received increased focus lately both in the public sector and ICT projects. But despite this increased focus, projects are still challenging. Several authors have researched the topic of ICT and project failures and many say this is related to lack of top management support, lack of communication, poor planning and unclear goals. Awareness and understanding related to risk and its management is also a factor that several author have pointed to.

The literature shows that risk and risk management is challenging and have been for more than 30 years. Risk has different definitions and in this study the following definition is used: Risk can be defined as an *"uncertain event or condition that, if it occurs, has an effect on at*

least one project objective". Risks can be calculated by using a formula, *Risk = Consequences × Probability.*

What is risk management?

Risk Management is the continuous process of identifying risks and responding to them in an appropriate way. Risk management can be defined as

"*a formal process that enables the identification, assessment, planning and management of risks".*

What is the purpose of risk management and how can it be performed?

The purpose of risk management is to *"select a course of action which provides an acceptable balance between likely benefits and exposure to risk"*. According to Kutsch (2008) the purpose of risk management is to *"manage risk in advance […] to respond to risks that may have a future adverse impact on the project outcome".* The four most common phases of a risk management process are risk identification, assessment, response planning and monitoring. Typically the risk management process consists of a variation of these processes (Taylor et al., 2012). The various standards for risk management all suggest similar processes and tools and techniques.

The literature in this chapter aims at creating an overall understanding of risk management in the Norwegian public sector. Further the literature aims at providing a background for understanding the research and the purpose of this study. It appears as there has been done research on risk management and critical success factors previously, but there is a gap in the research regarding barriers and enablers of risk management from a public sector perspective. The literature will be used for comparison and discussion with my findings in Chapter 5.

3. Research approach

This chapter presents the research approach used in this study. Firstly, I describe the research strategy and method. Then I present more details about the data collection method, interview, and the respondents of this study. This is followed by analysis. Validations and limitations to the study are discussed at the end of the chapter.

The aim of the empirical study is to develop a deeper understanding of the barriers and enablers of risk management in public ICT efforts. In order to get this deeper understanding I have used a qualitative research approach carried out by conducting 11 interviews in 9 organizations.

This research used a qualitative research approach. A qualitative approach is more in depth on an area of focus than a quantitative method, which focuses on superior response from many respondents. Dey (1993) describes the difference between qualitative and quantitative data: *"Whereas quantitative data deals with numbers, qualitative data deals with meanings. Meanings are mediated mainly through language and action. Language is not a matter of subjective opinion"* (p. 11).

The benefit of using a qualitative approach is that there are few limitations to the answer from the respondents. A qualitative approach is a flexible method, which emphasizes details and transparency. Transparency to the extent that the researcher has not decided completely on what he or she is looking for in advance. Within a qualitative approach there are different strategies to conduct studies; phenomenology, ethnography, narrative, case studies and grounded theory (Creswell, 2009). Case study is the most common research method within qualitative approaches, but grounded theory is chosen for this study. According to Oates (2006) a case study focuses on an event, organization, development project or a decision, whereas grounded theory seeks to generate theories that can explain concerns of the population and how to resolve them. The reason for choosing grounded theory approach is to go in depth on risk management and to develop a deeper understanding of barriers for risk management in public ICT efforts.

3.1 Grounded theory

Grounded theory has received increased attention over the past years when it comes to Information Systems research. There are several definitions on what grounded theory is, and Urquhart, Lehmann, and Myers (2010) has the following definition: *"Grounded theory is a qualitative research method that seeks to develop theory that is grounded in data systematically gathered and analyzed"*. Another definition pointed out by the same authors is *"the discovery of theory from data – systematically obtained and analysed in social research"*. This definition is the earliest definition of grounded theory and presented by the founders of the method, Glaser and Strauss in 1967 (Urquhart et al., 2010).

Grounded theory is a method that seeks to build theory based on field research and analysis. According to Oates (2006) *"grounded theory research should lead to theories that have practical relevance for the people in the situation studied"*. In other words, the results of the study, the theory, should make sense to the organizations I have studied.

According to Urquhart et al. (2010) grounded theory has four distinctive characteristics. The first characteristic is that the main purpose of grounded theory method is *theory building*. This characteristic relates to building theories and to have an understanding of the context. For me to be able to do this I have tried to acquire knowledge related to the context and topic, i.e. public sector and risk management.

The second characteristic relates to prior knowledge. The knowledge the researcher might have on the research topic should not lead to *preformulated hypotheses*. This is closely related to the first characteristics, theory building and not theory verification. For me to obtain this step, I have tried to separate previous research from my coding. This means that I have tried not to let my initial knowledge or the literature review influence the categories. However, I acknowledge that this to a certain degree is inevitable.

The third characteristic relates to *joint data collection and constant comparison*, meaning that analyzing and conceptualization of the data is compared with existing concepts to see if it can enrich other existing categories. The founders of grounded theory, Glaser and Strauss emphasized that *"the data collection, coding and analysis need to be done together because separating these operations might hinder the development of theory*" (Urquhart et al., 2010). In this empirical study I have collected data and coded them continuously and incrementally. I have revisited the data several times and new data have created new coding.

The final and fourth steps is called *slices of data* and reflects that different kinds of data will give me as a researcher a different view on how to understand a category. These new views should be used for further data collection. Collection data for this study was done over some weeks, and the new data was used to compare with existing codes, categories and concepts.

I have used grounded theory as an approach of structuring and analyzing the data gathered, and not as a complete method.

3.2 Data collection

The choice of method for collecting data will always have consequences for what results one gets in research. While quantitative research deals with large, random groups of participants, a qualitative research will use a narrow set of handpicked participants. For this research I have used qualitative semi-structured interviews as method for data collection.

3.2.1 Interviews

The main method of data collection for this study has been qualitative interview. According to Myers and Newman (2007) a qualitative interview is used in all kinds of qualitative research; case studies, action research, ethnographies and grounded theory. The authors mention three types of qualitative interviews; structured, semi-structured and group interviews. The Semi-

structured approach is the most commonly used (Myers & Newman, 2007) and is also used in this study. The characteristics of semi-structured interviews are that the researcher has prepared some of the questions before the interview takes place, but there is a need for improvisation. Normally the interviewer has developed an incomplete script.

According to Myers and Newman (2007) the qualitative interview is a good tool for data collection, but it is not always easy and straightforward to conduct. This is because the interview is an artificial situation in which a researcher usually communicates with a stranger. According to Myers and Newman (2007) the qualitative interview is *"one of the most important data gathering tools in qualitative research"*. Furthermore, Myers and Newman (2007) mention that the researcher is asking the interviewee to answer a set of questions under time pressure. To try to improve this situation, the interviewees got some of my topics and what I am looking for before the interview. This was sent out with the initial request for interview. By doing it this way I felt that the interviewees could be a bit prepared when we started talking and knew my anticipation. The biggest benefit of a qualitative interview is the openness (Kvale, 2007).

In total, I conducted 11 interviews and participated in one meeting with the public sector. I wanted to carry out the interviews in a setting that would be natural for the interviewee, e.g. the office of the interviewee. In an artificial setting the interviewee would give affected answers (Jacobsen, 2003), something I wanted to avoid and therefore tried to carry out all interviews in a natural setting. My initial thought was to collect data only through face-to-face interviews. As this proved to be difficult half of the interviews were done as face-to-face interviews and the other half done over phone. Since the interviews took place in a natural setting, I was prepared for interruptions from e.g. colleagues. Each interview was time boxed to 30-60 minutes. The first interviews took more time than the last, and this was due to my experience. The duration was also affected by how much information the respondent wanted to share.

For most of the interviews I conducted I was able to record using either my computer or a phone application. When recording the interviews I could focus more on the interview and not on the writing. During the interviews key words were written down so that these could be used for follow-up questions and to make sure the respondent answered what I was looking for. When the interview was done, I used the recordings for transcribing and later use the text for analysis.

3.2.2 Interview guide

As a background to the interviews, I developed a fixed set of open questions and topics. The interview guide can be found in Appendix A. When using an interview guide it is up to the researcher to make sure that all topics and questions are covered. This was ensured by always bringing the interview guide with me at all interviews. Whenever we had covered a topic I made a small mark in the margin of the document next to the topic.

The question in the interview guide was developed based on the literature review presented in chapter 2. In addition to the questions, the interview guide also included a small introductory part. Myers and Newman (2007) suggest that it is important to create a good atmosphere

when conduction the interviews. To create a good atmosphere there are several things one can do as a researcher. One thing is to think about the setting were the interview takes place. Another thing is to inform the interviewees about the study, who I am as a researcher, the goal of the research and so on. All interviews started by me telling about the aim of the study before moving on to the respondent.

The interview guide was revised several times. The first time after a review with my advisor and later after conduction some interviews. The first version of my interview guide contained too many questions, but after trying it out in practice I learned a lot and changed it to have only a few sets of open questions. Based on the revisions of the interview guide the interviews were easier to conduct. No question was eliminated, but I reformulated them to be broader.

3.2.3 Respondents

The selection of respondents is based on opportunity sampling through the researcher and supervisor's network. Opportunity sampling can also be called convenience sampling and is a part of the bigger term "non-probabilistic sampling", which reflects that respondents are chosen based on naturally occurring groups (Oates, 2006). This method of sampling has been criticized for being bias, but for this study the sampling was appropriate. The aim of the empirical study is to look at risk management in the Norwegian public ICT effort, and this will naturally create some bias. The selection criteria for this study were to find organizations where the concept of risk management could be studied in relations to ICT and/or interoperability projects. In addition to using my network, I attended a conference with DIFI early 2013 were I got in touch with some of the respondents. I also contacted some of the organizations that have a risk framework published and is included in my comparison.

3.2.4 Overview of respondents

I have interviewed representatives from eight different government agencies about their experiences with risk management. Furthermore, I interviewed two representatives from the private sector. All respondents, 11 in total, comes from Norway and they are all made anonymous. Three of the respondents come from the top 10 largest municipalities in Norway.

One organization is a public Norwegian company underlying The Ministry of Finance. The organization is working as an administrative organization, with focus on initiating, promoting and coordination reforms. The overall objective is to facilitate appropriate joint solutions in the public sector and make the governance easy in the various governmental agencies.

Another organization is a public Norwegian company also underlying The Ministry of Finance. The organization is working as an administrative organization, with focus on develop, interpret and administer the law.

A third organization is an independent foundation that works for safeguarding the environment, life and property. The core competence is to identify, assess and advise on how one should manage risks.

The fourth organization aims to strengthen the government's work in renewing the Norwegian public sector and improve the organization and efficiency of government administration. They

work to ensure that government administration in Norway is characterized by values of excellence, efficiency, user-orientation, transparency and democracy. They also aim to develop the organization and leadership of the public sector, with coordination among public authorities and services.

The fifth organization is an executive agency and competent authority subordinate to the Norwegian Ministry of Health and Care Services.

The last organization develops and operates many of the nation's most important registers and electronic solutions. Coordinating data in the public sector and providing advisory services are some of the tasks they perform.

The table below (Table 2) gives an overview of the respondents of this study and their role. The respondents are given a random number to obtain the anonymity. In addition a column for "sector" is presented to show if the respondents are from public or private sector and the "role" shows the role they have. "Type of interview" is either face to face or by phone and the last column gives an overview of the duration of the different interview.

Respondents	**Sector**	**Role**	**Type of interview**	**Duration**
Respondent 1	Public	Manager	Face to face	103 minutes
Respondent 2	Public	IT manager	Face to face	53 minutes
Respondent 3	Public	Project Manager	Call	28 minutes
Respondent 4	Public	IT Manager	Call	55 minutes
Respondent 5	Private	Consultant	Face to face	57 minutes
Respondent 6	Public	Advisor	Face to face	56 minutes
Respondent 7	Private	Consultant	Face to face	35 minutes
Respondent 8	Public	Project Director	Call	47 minutes
Respondent 9	Public	Manager	Call	34 minutes
Respondent 10	Public	IT Manager	Face to face	68 minutes
Respondent 11	Public	Head of department	Call	30 minutes

Table 2 - Respondents

3.3 Data Analysis

The data analysis process for this study is similar to process presented by Creswell (2009), see Figure 5:

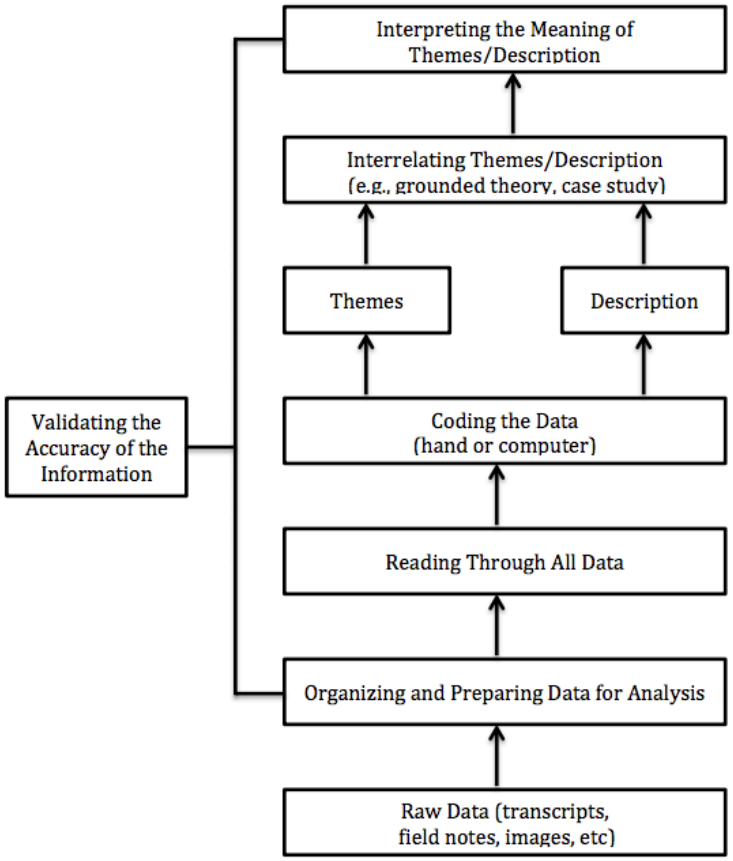

Figure 12 - Creswell Data Analysis Process (Creswell, 2009, p. 185)

All interviews were transcribed and the handwritten notes were added to the transcripts. All transcriptions were done in Norwegian, and citations have been translated for further presentation. I started transcribing interviews as soon as they were done and through this process I started coding into themes and categories. I tried to have an open mind throughout the process of analyzing data, and this is something that Oates (2006) emphasizes as important with grounded theory approach. For coding I used an application called Nvivo, a qualitative research tool. This was helpful because as the categories evolved I could easily change the names and move citations from one category to another. I started out with a high number of small categories, but ended up combining several categories. The result of this phase will be presented in chapter 5.

For a grounded theory approach to the data analysis there are three phases related to coding data: open, axial and selective (Oates, 2006).

Open coding relates to the initial process of labeling the data. It was during this phase that I ended up with a high number of categories. It is important to emphasize that the categories emerging is only found in the data and not from literature or pre-existing theories. Axial coding is the second phase and relates to moving to a higher level of analysis. This is where a researcher starts looking for relationships between codes. During this phase I incorporated several categories under broader headings and the outcome of the phase was less categories. The third and last phase is selective coding, which relates to refining and develop relationship between categories. This is where the theory building happens.

The analysis process is an iterative process and involves constant comparison. For any new code or category that I identified, I revisited previously coded data to see if I could improve the coding. This way the emerging theory is related to the empirical data (Oates, 2006).

The reason I have chosen to use Grounded Theory in my analysis is that little research related to my topic has been done before, and little research is related to the Norwegian sector. Therefore I found it reasonable to use a grounded theory approach and after the analysis compare it with existing literature collected from different domains.

3.4 Validation

According to Creswell (2009) validity can be defined as *"the researcher checks for the accuracy of the findings by employing certain procedures"*. There are several possible ways of ensuring validity to a qualitative research. This study has used the following strategies to add validity to the findings. Following a process like the one presented in Figure 4. By conduction the study at multiple organizations, triangulation of data was enabled and the theory was built based on several perspectives from the respondents. Further, to ensure quality of the study a third party who has not been involved in this study has reviewed the report to evaluate that the reasoning and conclusions are logical. Creswell (2009) argues that this can increase the validity of a qualitative study.

3.5 Limitations of the study

A possible limitation of this study can be that it is primarily based on semi-structured interview as a method of data collection. This can be a limitation because the only information I have is related to the informants' perception and experience on the topic. There is also a possible limitation related to whether I have interviewed the right respondents and if these respondents are representative for the public sector

Another possible limitation relates to me as a researcher, and that my task is to ask the questions and not discuss the respondents answers, experiences and statements. Since this is a topic I find very interesting, I have engaged in small discussions with the respondents. I have not gotten the impression that they saw this as something negative. Quite the contrary, I think this kind of discussion have had a positive effect on the results.

A third possible limitation is that all the data collection has been made in Norwegian, and the report is written in English. Some of the points made by respondents can be lost in translation. In order to prevent this from happening I have used friends to look over the translation and in some cases emailed the respondent to clarify and get an “ok” on the citations.

A last limitation relates to the analysis. The analysis was conducted by one person and it could be strengthening if two sets of eyes discussed the findings. This could increase the analysis and possible identify other findings than the ones presented in this study.

4. Results

This chapter provides a detailed description of the result of the study based on interviews done with 11 respondents. The study was conducted during the spring of 2013. The interviews were conducted between March 5th and April 10th 2013.

I start by presents the findings based on categories. The categories have emerged through the process of analyzing the data. Ten categories were identified and formulated through the analysis and use of Nvivo and are based on the enablers of risk management. The process of identifying categories has been iterative and started after the first interview. At first I had a high number of categories, but as the interviews were completed I revisited the categories several times and got a new view on them. This new view provided me with useful information and understanding of the relationship between the categories. Several categories where therefore combined.

The initial and final categories are displayed in the table below (Table 3):

Initial	Final
• Top management support • Requirements • Resources • Competence • Knowledge • Awareness • Understanding • Usefulness • Simplicity • Ownership • Communication • Value • Framework • Prioritize • Focus on importance • Visualize • Harmonizing • Definition • Agreement • Risk and interoperability	• Process • Management • Understanding • Communication • Awareness • Ownership • Competence • Resources • Harmonizing • Risk in interoperability efforts

Table 3 - Categories

The first two categories can be viewed as umbrella terms and consist of several related categories. The ten categories are, as we can see from the table above, process, management,

understanding, communication, awareness, ownership, competence, resources, harmonizing and risk in interoperability efforts.

My overall perception is that there is an increased focus on risk management in the Norwegian public sector. The majority of the respondents has been managing risk for a long time and has well-established methods. Others have recently started. Most of the respondents believe that risk management is essential and very important. A growing number of organizations are also getting certified, some within ISO. The impression is that risk management in general and risk as a topic has gotten more focus after July 22nd 2011, and this impression is shared among some of the respondents.

After a presentation of the findings and their corresponding categories, a short summary of the key findings is presented. The findings from this chapter can shed light on my problem statement:

What are the barriers and enablers of risk management in public ICT efforts?

Further, this chapter presents the findings from the empirical study. The chapter is structured and organized according to the ten categories that emerged through the analysis. At the end, a summary of the findings is presented.

4.1 Process

The use of process, method and framework is varying among the respondents. Most of the respondents use one or more frameworks, but 2 of the respondents do not have a framework for risk management. 3 respondents tell me that they use ISO 31000 and/or 27001/2 as framework. The remaining 6 respondents are using their own framework and adjust it to the need within different projects. All respondent are identifying the risks, defining risk element, set probability and consequence and making actions within their project. 10 of the respondents use a risk matrix based on probability and consequence. Some of the matrixes are presented in a 3x3 form, other in 4x4 or 5x5. The matrixes all consist of using green, yellow and red color to visualize the severity of the risks.

There are differences in how the respondents are defining the risk matrix. Some say that green is ok and they do not need to make any actions, other say that they need actions for all identified risks. For some of the respondents, risks that end up in the red area in the matrix means "stop", for other it means that the need to take immediate actions. The risk matrix is a vital tool that is continuously examined and updated in eight of the organizations.

One of the first respondent told be that *"the whole point of risk management is to prioritize"* (R5). A risk matrix is a tool that can help prioritizing what to do first and what to do next. *"It is key that you set it [risk matrix] properly so you can use it to set the right priorities"* (R5). No one has the recourses and capacity to do everything and prioritizing items correctly seems very important.

"When it comes to prioritization, we have an example of Sarbanes-Oxley. We see that for example the banking sector struggles with this, but also many from international companies that are subject to guidelines from the U.S. compliance requirements. Risk is important. And it is one of the biggest challenges because if you are not compliant with these things then your risk exposure increases. If you try to do everything it will cost too much and you will loose. Damned if you do and damned if you don't. It is therefore important to prioritize and do it right" (R7).

Respondent 3 pointed out another challenge when it comes to prioritizing. Different team members, managers and project owners may have different opinion on what is most important and should be given high priority. *"This is a new dimension that can provide additional challenges that must be risk management, clearly"* (R3).

Closely related to prioritizing we find a factor that the respondents mentioned as "focusing on what is important". In order to focus on the important aspects, one needs to make the right priorities.

"The more complex a project is the more important I think it is to use risk analysis as a management tool because it means that you can focus on the right things" (R11).

"One cannot let it become too complex, and should have a focus on what is actually important. […] What we are missing is focus in what we need, and what is important" (R6).

Too much information about the risks in a project can make it harder to manage and more difficult to sort out what is important. *"What I see many places is that risk managers have many intentions and desires, and they often have much information, but it is difficult for them to sort out what is important information"* (R7).

The respondents also point to defining risks correctly and precisely as an enabler. This relates to defining the risks and what you are going to analyze. *"It is important to defines what you are going to analyze"* (R11). Risks are often defined imprecisely and at a general level, *"the project can overrun or we cannot deliver want we want to deliver"*. According to Respondent 5 it is important to define the risks precisely and in a concrete way.

Two of the organizations say that visualizing the risk picture is very helpful for them. They use visualization a bit differently. Respondent 5 uses two matrixes to visualize status now and how the future will look if they take the planned actions. *"We often use two matrixes. This is the status now and if we can take the actions we have planned it will look like this. And then we can report it"* (R5). The other organization uses it to show the effect and usefulness of risk management, also called trend of trending. *"Every month, we show the development we have had in the areas of risk. This is visualized in a picture where we insert arrows to show where the risk area was when we started to work. Then you will see the gradual development of decline in risks"* (R11).

One of the biggest barrier of risk management is complex framework. One of the respondents called "complex framework" a classic barrier. *"Typically, if they have an dedicated risk resources they are going to make the framework for you. And then they make it most*

advanced. They want to do well and create it "after the book" – but then you end up not using it because of the level of ambition" (R5). Respondent 6 agrees and adds *"ISO 27005 is a very good standard for those who creates framework and guidelines, but it is maybe not a very good standard for those who want to use it. […] It is a risk that they boil away in complexity"* (R6).

What many organizations do is that they find a risk framework and adopt the entire framework thinking that this is what they need. And the result of this is that they have a heavy framework that they are trying to use, but all that is really happening is producing several documents and reports. The purpose of having a framework is to have some guidance and tools that can help managing risks. Several of the respondents pointed to simplicity as an enabler.

"To get it simple has been a challenge. And if we get it simple I think it has been much easier to manage" (R8).

"Simple is beauty" (R2).

"I think the most important success criteria in order to be successful with a tool like this is to set the bar low when starting to implement it" (R11).

"You need to learn how to crawl before you can walk" (R6).

Respondent 10 thinks the biggest barrier in their organization is lack of a framework and routines for risk management. *"The only thing inhibiting us from managing risks are lack of routines. It is not explicit written [in the project manual] that we are suppose to do risk management"* (R10). Also respondent 4 agrees with this. *"Lack of a standard for risk assessment inhibits. It makes it limited. If you have a template of how things should be done this helps enable"* (R4).

The table below (Table 4) gives an overview of the barriers and enablers from this category:

Barrier	Enabler
• Complex framework	• Simple framework • Visualization • Opportunity for prioritization

Table 4 - Process findings

4.2 Management

Management involvement is another topic that several respondents pointed out. Support from the top management is a critical success factor and it is seen as a vital impetus. The respondents feel that management needs to focus on risk management and demonstrate it to the employees. They feel the need to be measured on risk management just as any other activity they do. In some cases the employees keep on reporting on risk, aggregating the risk to the management and never hear anything back. One respondent said that when this happens

they will eventually stop reporting. Risk management is about managing and the management needs to show that they are using the information reported to manage the risks.

"Something we have seen recently is that you need to have top management support, at least when the project involves other parties" (R10).

"Most of all, risk management implies that someone is managing. That the management is managing. And this means that they need to understand risk." (R6).

"It is a management challenge. The main responsibility lies with the manager, of course. If I, as manager, cannot see the usefulness of this, and does not have the ability to manage it and I do not expect the employees to use the tool – then nothing happens. So this responsibility lies at the management level" (R11).

Six respondents highlight that one should focus on the usefulness when it comes to getting employees committed with risk management. If the usefulness is not highlighted, people might see risk management as just another task they have to do because someone said so, and not because it is valuable. Respondent 4 suggested to make a conference where people can share their experiences and know-hows when it comes to risk. This would mean that someone needs to take a step forward and talk about what went wrong in a project and others demonstrating that they had a lot of help from risk management.

"And every month, we present the development we have had in the areas of risk - we visualize it in a picture where we insert arrows that show where the risk areas were when we start work. Then you see the gradual development in decline of risk. And it is quite fun for people to deal with because when they see that it is useful" (R11).

" I find it important to be able to present success stories early in a project" (R8).

"We need to focus on the usefulness […] and demonstrate the usefulness" (R4).

"Someone needs to impose requirements about it - it is suppose to be a tool for management" (R3).

Some respondents say that it is important that identifying and managing risks is something that is required by management. If no one requires that risk management is something you have to do, then the most likely scenario is that risk management is not being conducted. But when requiring, it is also important to communicate *why* they need to report and not only tell them to report. When doing this, risk management will become an active tool for managing.

"Every project owner and project manager needs to require to demand risk and risk management as a part of project implementation" (R8).

Another respondent pointed out that imposing requirements regarding risk management would make decision-making easier. *"To be good at imposing requirements that makes you better at making decision is key. […] If you are very clear about what to do and why, I think that will help"* (R7).

"The government requires that we should have a risk management process. It is a common requirement in the government today that big important projects and interoperability efforts are risk managed. That is important" (R3).

Other respondents think there is a great line between imposing requirements and making risk management as compulsory exercise. If management requires that the team perform risk analysis, it should be because they want the information. *"You do it as a compulsory exercise, but you don't use it for anything. If there is a point of risk management is it to take actions"* (R5).

The table below (Table 5) gives an overview of the barriers and enablers from this category:

Barrier	Enabler
• Lack of top management support	• Demonstrate usefulness • Impose requirements

Table 5 - Management findings

4.3 Understanding

Having an understanding for risk management and what risk can do to your project is essential for the project and the project team. Several respondents pointed this out. People without this understanding might see risk management only as a time consuming task. One respondent told me that there has been lack of understanding of the value of risk management in his organization, but that this has turned now and that more and more people have a better understanding.

"I believe, that one of those things that are missing is simply understanding among the decision makers about what risk is" (R7).

"What inhibits risk management is the lack of understanding of the value of it. […] People who understand the value of risk management, I think that is important" (R8).

One respondent says that the management also needs to have an understanding of the value of Risk Management. This issue does not only lie at the employees.

4.4 Communication

"We have a critical release and with this we see that risk management and communicating the risk factors to the internal management but also to the department, have been an important tool (R3).

Communication is an import aspect of managing risks. If new risk emerges it is important to communicate the changes to the rest of the team and the managers that makes the decisions. And this should be a topic of every project meetings. Are there any changes? Is there anything

that potentially can harm us? Good communication is viewed as an enabler and something that can reduce the risks in a project.

"Don't under communicate the risk, because we gain nothing from doing that. Because the risk then becomes like a boomerang and hits you" (R10).

Another aspect of communication is to have management that care. One of the respondents told me that they have a manager that is concerned with risk.

"He talks risk and communicates the risks. And discusses the risks. I find that he is very good at communicating how he sees risk" (R7).

4.5 Awareness

Having an awareness of risk and what risk can do you your organization and project is something that several respondents pointed out. One responded said that we find evidence of organizations having risk issues and challenges in the daily paper

"Clearly, one gets the impression that [the company] has not had an awareness to risk management because they have not taken any action in relation to what obviously is a red risk profile" (R1).

Another respondent points out something similar

"I think the keyword of this is awareness. […] because if you knew something and did not take action, then you most likely will be caught by media" (R7).

The same respondent also pointed out that the principle is just to have awareness of what risk is and what you can do to manage, minimize and/or mitigate the risks.

Another respondent pointed out that if you are aware of the risks involved in you project, addressing them takes almost no time. If you spend 2 hours every other week or includes risk as a part of project meetings it takes almost no time.

"It takes almost no time, but they must be aware" (R5).

Respondent 2 did not mention awareness during the interview, but I got to see the organizations project manual and awareness is one of the things mentioned. *"High awareness of developments in the project risk profile during project execution increases the probability of project delivery"* (Project Manual, R2).

4.6 Ownership

Creating ownership and making sure everyone feels included in the project is also an enabler of risk management. This is something the project manager needs to try to enable and try to incorporate risk thinking across the team.

" To establish ownership among everyone involved in the project is important. […] It is also important that the person responsible for the project ensures that the project incorporates risk thinking in the project group among all participants so that it not only becomes an exercise that the mangers do for themselves – it is the ownership one must try to establish" (R8).

Having ownership is also important to be able to have better value of the tool. *"The greater ownership and understanding you have for what has been done, the greater advantage one have from the tool [risk management]. […] There should be room for discussions because this helps with creating ownership and a common understanding"* (R11).

4.7 Competence

Having competence with risk management is something several respondents believe is important. This factor relates to having competence to what risk is, what tools are available and how to use them. The respondents also highlights that it is important to have competence on what a risk analysis is and how to perform it.

"The challenge is mostly on competence. Competence in terms of understanding what risk is and how to conduct [an assessment]*"* (R6).

"It is important to have one person with good competence on what risk analysis is when we start to work" (R11).

Another point made by Respondent 11 is that the project team conducting the projects should have different competence. *"It is important that the team doing the work have different competence and different roles"* (R11).

The competence factor is also related to how well you can be able to manage risk and Respondent 1 is convinced that having good competence will enhance the opportunities. *"Having good competence will enhance the opportunities, I am convinced"* (R1).

Competence is something that easily can inhibit the work with risk management. Respondent 1 thinks that there is a lack of competence for risk management in the public. *"I am a bit worried whether managers in the public sector are competent or not in this management area. We have evidence that managers are not competent. But I believe that it is variable competence among top management in the public sector when it comes to risk management"* (R1).

Respondent 5 does not believe competence is as important as other respondent. *"Competence is not the barrier I put at the top of my list. Risk management is not* that *difficult. It is just to have a method and follow that"* (R5).

4.8 Resources

Lack of resources is also a barrier to risk management. Without resources risk management will not be carried out. Unfortunately there seems to be a lack of resources in the public sector, and the companies that have the resources seem to have limited resources.

"He has no resources, unfortunately. It is so limited. It is a bit sad that resources are so limited" (R1).

"When a big business like [organization] only has 8 people working with risk then it goes without saying that small organizations do not have sufficient resources to do this" (R6).

Other respondents see this factor differently. Respondent 11 thinks that risk management and risk analysis will help ensure the right use of time and resources. And points out that this is why risk analysis is a good tool.

4.9 Harmonizing

Harmonizing is closely related to risk methodology and to achieve agreement. Having methods, frameworks and tools that are harmonized is deemed as important amongst some of the respondents. Having many different ways of working and managing risks is a challenge.

Respondent 7 have been involved in many projects where this challenge is applicable. *"They have* many *ways of working and it might work, but the issue is that they have many different ways of working. It has not been harmonized. I have had several meetings this week and they all have that challenge"* (R7).

Respondent 7 is not the only one who has mentioned that this is a challenge in the public sector. *"They [employees] can sit lined up at the office, all running different risk methodology and all complain that the management do not understand. What they adequately fail to do is to coordinate. […]. They must ensure the harmonizing"*. (R6)

Respondent 6 also points out that a key element within risk methodologies and tools it so get it harmonized. *"To be able to get harmonization risk methodology, tools and how you do it. We consider this as a key element"* (R6). Further, Respondent 6 thinks that harmonizing is easy and not complicated. *"It is not complicated as most risk methodologies are based on the same structure. Its just that they make their own versions " (R6).*

Respondent 11 also agrees on the importance of harmonizing. *"It is important with harmonizing"* (R11).

4.10 Risk and interoperability

Risk management in relations to interoperability has different perceptions among the respondents. Risk is also managed differently among the respondents when it comes to

interoperability projects. The majority of the respondents think that managing interoperability projects are more complex and challenging than other types of projects.

Respondent 5 thinks that interoperability projects are challenging and that it is more important to have control on the risks *"Much more challenging, and the more important to have control on the risks"* (R5). This idea is shared with respondent 9. *"It is definitely much more complex. You have several participants, with different cultures in different agendas and different goals"* (R9).

Many of the respondents emphasize that it is more important to have a mutual understanding, agreement and perception of risks when it comes to interoperability projects. *"It is more important that everyone has the same understanding, the same perception of how risks are communicated"* (R11). *"The difficulties lie in coordination, and to do it equally across units and organizations"* (R3).

Both respondent 6 and respondent 9 think that interoperability projects are complex, much more challenging and time consuming. *"It is very much one should agree on"* (R9). Further respondent 9 points out that *"it is very different, and much more challenging with this interoperability"* (R9). *"They have their things they want to focus on, and with more people with different experiences getting together to create something, things will take a long time"* (R6).

Respondent 3 is the only respondent who pointed out that they manage interoperability projects just as any other projects. *"We do not manage it differently – it is a project that is managed like any other."* (R3)

4.11 Summary of findings

As this chapter demonstrates, the way risk management is being practiced in the public sector is corresponding to frameworks and standards. This chapter also presents several barriers and enablers to risk management. A summary of the findings can be found in the table below (Table 6):

Barrier	Enabler
• Complex framework • Lack of top management support • Lack of understanding • Lack of competence • Lack of resources • Lack of harmonization	• Simple framework • Visualization • Opportunity for prioritization • Demonstrate usefulness • Impose requirements • Communication • Awareness • Creating ownership

Table 6 - Summary of findings

When reviewing what the respondent said about risk management in interoperability efforts we see that those projects are more complex which gives the need for more management. It is increased important to have shared goals, focus, understanding and perception of risks in the projects.

5. Discussion

This study focus on understanding risk management and the challenges related to risk management. The findings from the interviews were categorized and formulated into ten categories of enablers and barriers of risk management in the public sector. These categories made the basis for the result chapter (Chapter 4) and will be further used in this chapter. This chapter reviews the findings from the empirical study and discusses them in the light of the thesis problem formulation and research question. The results will be discussed in light of the literature review.

This master thesis has the following problem formulation

What are the enablers and inhibitors of risk management in public ICT efforts?

Further, the problem formulation was divided into the following research question

- *What is risk management?*
- *What is the purpose of risk management and how can it be performed?*
- *What characterizes enablers and inhibitors of risk management?*
- *What characterizes risk management in interoperability efforts?*

This chapter is structured based on the research questions, where I start by presenting answer to research question 1 and 2. The categories from the result chapter will be discussed under research question 3 and 4.

5.1 Risk management

This section seeks to answer research question 1 and 2.

- *What is risk management?*
- *What is the purpose of risk management and how can it be performed?*

As seen in chapter 2, literature review, Risk Management has many different definitions. Two definitions were used in this study. One definition used is *"Risk management is a formal process that enables the identification, assessment, planning and management of risks"* (Merna & Al-Thani, 2008). The other definition is *"the entire process of actively considering risks in project context"* (Powell & Klein, 1996).

Having a risk management strategy is necessary to survive in today's market (Merna & Al-Thani, 2008). Organizations and technology changes rapidly and it is becoming more difficult to identify risks and recognizing the unusual. There are several benefits of risk management and applying risk management early in a project will increase the chance of

better dealing with risks (Hulett, 2012). The purpose of risk is to identify the risk in advance and select a course of action that is acceptable.

As seen in Chapter 2,3 there is a variety of existing risk management standards and they are all corresponding. Typically the risk management process consists of a variation of the same phases. The four most common phases of a risk process are risk identification, assessment, response planning and monitoring. The comparison of standards shows that there are many similarities in the existing standards and that the majorities are based on the same standards, AS/NZS and ISO.

5.2 What characterizes barriers and enablers of risk management?

In this subsection I will discuss the main findings related to the barriers and enablers from the empirical study. The findings will be discussed in relations to the literature review. The structure outlined in chapter 4 will be applied further.

5.2.1 Process

As seen in the analysis, nine out of eleven respondents applied Risk Management in some format similar to the best practice processes. In those nine respondents organizations, a process of identification and response took place in a similar way to the process suggested by ISO and PMI. In the last two organizations no formal risk management process was applied.

As seen in the literature, a risk management process is beneficial because it seeks to ensure that information about risks are identified, processed and reported adequately. The benefit of using a risk management process is that it will help the organization make risk management an integrated part of the management process and risk management can become a regular activity. According to Powell and Klein (1996) the purpose of risk management is to *"select a course of action"*.

The high number of different frameworks and standards that exists implies that having a framework is important. And this is supported by the empirical data. Nine of eleven respondents have well-established risk management processes. The last two organizations lack a framework. Several respondents pointed out that having a framework helped managing risks. One respondent in particular, pointed out that *not* having a framework was a huge barrier for them. Both respondent 4 and 10 agree upon that not having a framework is a barrier for risk management. Respondent 10 made a comment on this by saying *"the only thing inhibiting us from managing risks are lack of routines"*.

The reason for the lack of a framework, I think, is that the two organizations are smaller than the other nine and that they therefore lack resources. My impression from the interviews was that they also lack some understanding to what a risk is and what the benefits of having a risk management framework is. I base this statement on the fact that the only barrier for them is that they do not have routines, and if that is the case, they would benefit from employing a formal Risk Management Process.

When it comes to the content of the framework several respondent agree that you need to set the bar low, or else it will be difficult. Literature has shown that despite of many years of research risk management still remains a challenge, and a complex framework can create resistance. Respondent 5 called complex framework a typical barrier, respondent 2 agrees and states that *"simple is beauty"*. As mentioned, the majority of the respondents have a framework corresponding ISO or PMI. I think the reason for the similarities relates to the purpose of risk management, identifying and mitigating risk in advance, and there are only so many ways of doing it. This might also be the reason why most of the framework also is so similar, it is a prudent way of managing risks and it works.

The most common tool amongst the respondents is a risk matrix. There is a difference in the way that the respondents presents and define the matrix. Some say that green is ok and they do not need to make any actions, other say that they need actions for all identified risks. For some of the respondents, risks that end up in the red area in the matrix means "stop", for other it means that the need to take immediate actions. As seen in the literature, risks that end up in one the red area of the risk matrix are considered to be critical. Dependent on the number of risks in the red area and the complexity of the project I would say that one should take actions and possible stop the projects.

Using a tool like risk matrix can help prioritize activities in your projects. Several respondents pointed out that *"the whole point of risk management is to prioritize"* and that a risk matrix is a good tool for that. This is supported by the literature. The matrix allows organizations to prioritize the risks (PMI, 2009). The respondent pointed out that this is a good tool because no one has the resources to do everything and prioritizing seems to be important and necessary. *If you try to do everything it will cost too much and you will loose. Damned if you do and damned if you don't. It is therefore important to prioritize and do it right"* (R7)*"The more complex a project is the more important I think it is to use risk analysis as a management tool because it means that you can focus on the right things"* (R11). This suggests that using a risk matrix and prioritizing the risk is important and will make you prepared for any occurring risks.

5.2.2 Management

According to previous research (Kappelman et al., 2006; Tesch et al., 2007; Wibowo & Yuwono, 2008) top management support is an important enabler for risk management. Lack of or inadequate top management support can have a big impact on projects. Firstly, the management needs to be open about their thought and ideas related to risk. Secondly, employees tend to do what they believe management wants them to do. If the employees feel that management is not focused on risk management, then their focus will also be on something else.

Several respondents agree with what the literature says and Respondent 6 illustrates this by saying that *"risk management implies that someone is managing. That the management is managing"*. In order for someone to manage, it indicates that there needs to be support from top management.

Several respondents also pointed out that management need to impose requirement in order to be better at making decisions and mitigating risks. Setting some expectations that the employees can conduct. *"If you are very clear about what to do and why, I think that will help"* (R7). Having a risk management framework that describes what to do and how will be beneficial. Then the top management can use the framework and through the processes receive useful information for better decision-making. The employees will also know what to do, how to do it and why they are doing it.

Top management support is also closely related to usefulness, something that also was pointed out by several respondents. And the findings indicate that it is the management's responsibility to demonstrate the usefulness. Respondent 4 thinks we need to focus on the usefulness in order to get more people focused.

5.2.3 Understanding

According to previous research (Hopkinson et al., 2008; Hulett, 2004; Intaver, 2004), there is a lack of common understanding about risk and risk management. Hulett (2004) argues that businesses and organizations do not understand how risk contributes to results. Intaver (2004) describes that managers and businesses do not believe in risk management being beneficial and therefore lack understanding. Hopkinson et al. (2008) suggest that a *"clear understanding of risks is essential"*.

At an overall level, the respondents agree with this. Most of the respondents have a clear understanding of risk and risk management. One respondent told me that there had been lack of understanding in his organization, but that they worked towards establishing understanding amongst the employees and management. The overall impression I got was that employees in this organization now have better understanding of risk and the value of risk management.

During the interviews I also got the impression that many see risk management as a time consuming task and don't understand the true value of it. Responded 8 also thinks that the lack of understanding of the value is a barrier to risk management adds *"people who understands the value of risk management, I think that is important"*.

5.2.4 Communication

Several authors have pointed at communication as an important factor for risk management (Boehm, 1991; Grabowski & Roberts, 1999; Harner, 2010; Hwang et al., 2004; Kappelman et al., 2006; Neimat, 2005; Whitmore & Choi, 2010; Williams, 2004). In addition, multiple risk standards have included communication as one of the iterative phases.

All respondents mentioned communication as a critical and important factor for risk management. Several of the respondents had success stories to tell related to communication. Respondent 3 just had a critical release and communicating the risk factor was an important tool. Respondent 11 also had a release and with good communication they managed to release it earlier than expected. All these are examples of the importance of communication.

Respondent 10 emphasized that it is better to communicate too much, than too little. Because under-communicating risk will only do more harm than good. *"The risk then becomes like a*

boomerang and hits you". I heard a quote once that relates well to the issue of communication. *"I don't mind bad news, I receive them every day, but I do not like surprises"*. I think this quote supports that one should not under-communicate, and if you possess information that possibly can harm the project it is best to tell.

5.2.5 Awareness

Awareness is a factor that was emphasized by the respondents and is ranked high on the list presented by Wibowo and Yuwono (2008). I believe that awareness and understanding are related factor, but understanding relates to realizing the value of risk management whereas awareness relates to realizing what risk can do to your project and organization.

Having a risk aware culture is according to literature (Hopkin, 2012; Wibowo & Yuwono, 2008) related to understanding. Having risk awareness, combined with understanding and good communication can enhance risk management. This was also pointed out in Respondent 2's Project Manual: *"High awareness of developments in the project risk profile during project execution increases the probability of project delivery"*.

Respondent 7 pointed out that one should have awareness of what risk is and what you can do to manage, minimize and/or mitigate the risks. The respondent also pointed out "*the keyword of this is awareness. […] because if you knew something and did not take action, then you most likely will be caught by media"*. We can see that this is related to communication and sharing information and if a team member knew about the risk it is better to share it, than to ignore or avoid it.

5.2.6 Ownership

Ownership is a factor that is perceived differently in the literature and the respondents. In the literature we have seen that ownership is related to management, and that the ownership should be allocated to management. According to R. J. Chapman (2011) risk management is most effective when *"ownership of risk is allocated to an appropriate senior official"*. But the findings from the study suggest that ownership among all involved is important, meaning a form of employee ownership rather than management ownership. "*To establish ownership among all involved in the project is important"* (R8).

Respondent 11 also points out the importance of establishing ownership among the project team, and points to being open for discussion. "*There should be room for discussions because this helps with creating ownership and a common understanding"*.

From this we can see that management ownership and employee ownership is important. And establishing ownership among the employees is a manager's job: *"It is also important that the person responsible for the project ensures that the project incorporates risk thinking in the project group among all participants"* (R8).

5.2.7 Competence

Competence and knowledge is closely related to each other and I have therefore combined those categories. Several respondents pointed out that having competence is important. This enabler is also found in the literature (Bakker et al., 2009; Braig et al., 2011; Faisal et al.,

2006; Sumner, 2000). The respondents points out that having good competence will enhance the opportunities of risk management and that it is important that different team members possess different competence (R1 and R11).

The respondents discussed that having the right competence as a challenge. *"The challenge is mostly on competence"* and *"It is important to have one person with good competence"* are two of the comments made by the respondents. My impression was that there is a lack of competence in the public sector and Respondent 1 also indicated this by saying *"I am bothered a bit whether managers in the public sector is competent in this management area"*.

5.2.8 Resources

Lack of resources is a barrier and challenge pointed out by several respondents. Unfortunately, this barrier seems to be a challenge throughout the public sector. *"When a big business like [organization] only has 8 people working with risk then it goes without saying that small organizations do not have sufficient resources to do this"* (R6).

The literature also points to lack of resources as being a challenge. Lack of enough staff or staff with the right skills is on top of the list presented by Tesch, Kloppenborg, and Frolick (2007). Also Hofmann (2010) presents that the number one challenge for companies is lack of risk management dedicated staff and personnel. This was also pointed out by Respondet 1. *"He has no resources, unfortunately. It is so limited. It is a bit sad that resources are so limited"* (R1).

Respondent 11 thinks that one can use risk analysis to ensure the right use of time and resources. By ensuring the right use of time and resources one can avoid the challenge with lack of resources.

5.2.9 Harmonizing

Harmonization of methods and standards is an enabler that emerged through several interviews and an enabler I did not view as important at first. But after completing my comparison of the different frameworks and at the same time carrying out the interviews, I deemed this as more and more important. The variety of frameworks indicated that the there is a need for frameworks, but also that it is time to start harmonizing. From the comparison we see that the ISO standards, the Australian and New Zealand standard and the standard from IRM are almost identical. Similar to those three are PMI's standard.

Respondent 7 pointed out that harmonizing is challenging in the public sector; *"They can sit lined up at the office all running different risk methodology"*. Most of the risk standards and methodologies are based on the same principles and this indicates that harmonizing should not be a difficult task and that the problem lies in that everyone is making their own version of the frameworks.

The number of different risk standards also indicates that it can be difficult to chose which one to use, and that organizations therefore creates their own version. This is something that was pointed out in a paper by DIFI stating *"We are a bit confused here when DFØ, DIFI and*

The Norwegian Data Protection Authority publishes different guidelines in the same topic. What should we use?" (DIFI, 2012).

It is not only the standards that should be harmonized, but also the process of definition, identification and response. This way the process could become straightforward and easier manageable. This implies that harmonizing has the power to simplify, make the methods reusable across organizations and sections, and create better management. The aim of harmonizing should be on facilitating a common framework and processes for managing different areas of the business. This implies that a harmonization will create a foundation for better understanding of enterprise-wide management and highlight possible challenges for interoperability.

5.3 What characterizes risk management in interoperability efforts?

The fourth and last research question relates to risk management in interoperability efforts. As literature has demonstrated, interoperability is challenging and complex. One factor that makes interoperability projects more complex than others is that two or more organizations have to agree upon different factors. The different organizations might have different goals, different risk management culture and other differences (Adams et al., 2007; Misuraca et al., 2011).

With all the different factors that comes into play, this suggests that interoperability is done differently and can become challenging. The majority of the respondents support this. Respondent 5 emphasized that interoperability projects are challenging and it is increasingly important to have control of the risks. *"Much more challenging, and the more important to have control on the risks"* (R5).

Communication is previously mentioned as an enabler for risk management both from the view of literature and respondents and it is also important within interoperability. Understanding and perception is also mentioned previously and is increasingly important in the interoperability context. *"It is more important that everyone has the same understanding, the same perception of how risks are communicated"* (R11). All of this indicates that the complexity of interoperability projects suggest that one need to emphasize on the general enablers.

"They have their things they want to focus on, and with more people with different experiences getting together to create something, things will take a long time" (R6). This quote indicates that there is a need for a longer startup phase where one can agree upon the project executing. Things that need to be agreed upon are the goal of the projects, how risks are being communicated, and sharing each other's perception on risk culture and risk understanding. *"The difficulties lie in coordination, and to do it equally across units and organizations"* (R3).

My initial perception was that there is a need for increased risk managing in interoperability efforts and it seems that this perception is shared with the respondents. Another perception I

had was that interoperability projects needs to be managed differently than others. None of the respondent supported this explicit, and Respondent 3 pointed out the opposite, that managing interoperability projects are not different from other projects. *"We do not manage it differently – it is a project that is managed like any other"* (R3).

6. Conclusion

This thesis has through a literature review and 11 qualitative interviews investigated challenges of risk management in practice and are based on the Norwegian public ICT effort. The aim of the study is to answer the following research question:

What are the barriers and enablers of risk management in public ICT efforts?

The study shows that Risk Management in public ICT efforts can be challenging and complicated. A number of barriers and enablers were identified and categorized. The categorization was a result of the analyses, carried out with a grounded theory approach. The main categories are process, management, understanding, communication, awareness, ownership, competence, resource, harmonizing and risk management in interoperability. The first two categories are deemed as umbrella terms and consist of a combination of several smaller categories. The first category was used to shed light on barriers and enablers related to the execution of risk management. The second category relates to management and that management needs to be involved in managing risks.

There is a degree of consistency between the literature and practice. The literature review revealed a long list of key success factors, barriers and enablers and some of them were also found through the interviews. However the interviewees also pointed to other important issues not found in my literature review. This could be caused by the interviewees taking a more practical approach or that they simply state pains experienced on their current projects. Two enablers found in the empirical study but not in the literature are simple frameworks and visualization.

This study shows that the lack of a framework is not the sole reason for risk management to be challenging, but also lack of support from management offers challenges. As the table below (Table 7) presents, this study has revealed several enablers and barriers for risk management in public ICT efforts. The study concludes with the following barriers and enablers of risk management in public ICT efforts.

Barrier	Enabler
• Complex framework • Lack of top management support • Lack of understanding • Lack of competence • Lack of resources • Lack of harmonization	• Simple framework • Visualization • Opportunity for prioritization • Demonstrate usefulness • Impose requirements • Communication • Awareness • Creating ownership

Table 7 - Results

When managing risks in interoperability efforts it is increasingly important to agree upon different factors. The study shows that it is important to have mutual understanding of the

risks in the project, shared focus and goals, and shared perception of risk communication. The study also shows that it is more difficult to coordinate interoperability projects, than for internal organizational projects. It is also challenging to manage equally across units and organizations.

It is also important to emphasize that the findings are not set answers, but rather a first attempt at a theoretical understanding of issues related to risk management in the Norwegian eGovernment settings. This understanding has implications of what can be done better in practice, and further research.

6.1 Implications for research

This study contributes to research on the topic of risk management, and contributes to increased understanding and knowledge of risk management in practice related to Norwegian public organizations. Considering that the number of respond is only 11, this study can create a foundation for further research on the topic of risk management in the Norwegian public sector. One could do a study in similar organizations to the ones studied and examine the topic in a broader sense. The study can be carried out by examine more respondents from the public sector and focus on only challenges or only the risk management process.

One could also conduct further research on risk culture and how to increase a good risk culture. This in order to fix the shortcoming represented by the barriers and to take advantage of the opportunities represented by the enablers. Organizational theory and theory related to change management could be looked at. This is closely related to by study, but lies outside of my scope.

Further research is recommended to increase the knowledge and understanding of risk management in the Norwegian public sector. Further research could also validate my findings.

6.2 Implications for practice

During my work with this study, I have identified several interesting findings that can serve as important for organizations that wants to adopt risk management or organizations that have adopted risk management. The results from this study has the potential to provide organizations, managers, standardization bodies and developers of standards and frameworks with useful information regarding barriers and enablers that affect the risk management success. It is advisable for organizations to look at the barrier and enablers presented in this thesis to get an understanding of challenges related to risk management. The results from this research can create value for practitioners by raising awareness of the importance to change the organizational culture when managing risks. It can also give risk management more attention.

As a result of the findings, the following recommendations can be made regarding organizations adopting or working to improve their risk management process:

- Management should be aware and focus on all the enablers and barriers to obtain greater benefits when it comes to risk management
- Management and executive support is vital to achieve risk management success
- Focus and barriers and enablers to reduce the impact of barriers and to exploit and strengthen the enablers to succeed in their work
- Demonstrate the usefulness and benefits of risk management to ensure a good risk culture
- Managers should pay attention to the increased challenges of interoperability

The following recommendations can be made regarding standardization bodies and developers of standards and frameworks:

- Frameworks, standard and guidelines need to be easy to understand and implement to gain user acceptance
- The value of risk management must be identifiable
- Frameworks, standard and guidelines should facilitate good communication, information sharing and visualization
- Use the list of barriers and enablers as a guide for focusing the attention on effective risk management and to assess improvements in frameworks

7. References

Adams, Barbara D., Waldherr, Sonya, & Lee, Kenneth. (2007). Interoperable Risk Management in a Joint Interagency Multinational Environment: On behalf of DEPARTMENT OF NATIONAL DEFENCE.

AIRMIC, ALARM, & IRM, . (2002). A Risk Management standard.

Alleman, Glen B. (2002). Information Technology Risk Management. The concept of Risk, Its Management, and the Benefits to an IT Project.

Australian/New Zealand Standard. (2009). Risk management—Principles and guidelines.

Bahill, Terry, & Smith, Eric. (2009). An Industry Standard Risk Analysis Technique. *Engineering Management Journal, Volume 21*(No. 4), 14.

Bakker, Karel De, Boonstra, Albert, & Wortmann, Hans. (2009). Does risk management contribute to IT project success? A meta-analysis of empirical evidence. *International Journal of Project Management*, 11.

Bélanger, France, & Carter, Lemuria. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems*, 11.

Boehm, Barry. (1991). Software Risk Management: Principles and Practices. *IEEE Software*.

Braig, Stephan, Gebre, Biniam, & Sellgren, Andrew. (2011). Strengthening risk management in the US public sector.

Carlos, Tom. (2008). Reasons Why Projects Fail.

Chapman, C., & Ward, S. (2007). *Project Risk Management: Processes, Techniques and Insights*: John Wiley & Sons.

Chapman, Robert J. (2011). *Simple Tools and techniques for enterprise risk management* (Second edition ed.): Wiley Finance.

Choudhari, R. D., Banwet, D. K., & Gupta, M. P. (2005). Risk Profile in E-governance Project. *3rd International Conference on E-Governance*.

Choudhari, R. D., Banwet, D. K., & Gupta, M. P. (2006). Identifying Risk Factors in for E-governance Projects.

Chulkov, Dmitriy V., & Desai, Mayur S. (2005). Information Technology Project Failures. Applying the bandit problem to evaluate managerial decision making. *Information Management & Computer Security, 13*(2), 9.

Cioaca, Catalin. (2011). Qualitative Risk Analysis Methods in Aviation Projects. *Journal of Defense Resouce Management, No. 1*.

Cohn, Mike. (2006). *Agile Estimating and Planning*: Prentice Hal.

Conrow, Edmund H. (2000). *Effective Risk Management: Some Keys to Success*. Reston, Virginia: American Institute of Aeronautics and Astronautics.

Creswell, John W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*: SAGE Publications.

Dey, Ian. (1993). *Qualitative data analysis. A user-friendly guide for social scientists*. London and New York: Routledge.

DFØ. (2005). Risikostyring i staten. Håndtering av risiko i mål- og resultatstyringen.

DIFI. (2010). Risikovurdering - en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.

DIFI. (2012). Styringssystem for informasjonssikkerhet. Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002. http://www.difi.no/filearchive/difi-rapport-2012-15-styringssystem-for-informasjonssikkerhet.-erfaringer-og-anbefalinger.pdf

DIFI. (2013). Veiviser skal gi bedre offentlige IT-prosjekter. from http://www.difi.no/artikkel/2012/12/veiviser-skal-gi-bedre-offentlige-it-prosjekter

Duggan, Orna. (2006). Enterprise risk management - the challange for the public sector. *Accountancy Ireland, Volume 38*(Issue 4), 3.

Faisal, Mohd Nishat, Banwet, D.K., & Dhankar, Ravi. (2006). Supply chain risk mitigation: modeling the enablers. *Business Process Management Journal, Volume 12*(Issue 4), 19.

Flak, Leif Skiftenes, Dertz, Willy, Jansen, Arld, Krogstie, John, Spjelkavik, Ingrid, & Ølnes, Svein. (2009). What is the value of eGovernment - and how can we actually realize it? *Transforming Government: People, Process and Policy, Volume 3*(Issue 3), pp. 220-226.

Gottschalk, Petter, & Solli-Sæther, Hans. (2008). Stages og e-government interoperability. *Electronic Government, An International Journal, Vol. 5*(No. 3), 11.

Grabowski, Martha, & Roberts, Karlene. (1999). Risk Mitigation in Virtual Organizations. *Organization science, Volume 10*(Issue 6), 18.

Harner, Michelle M. (2010). Barriers to effective risk management.

Hillson, D., & Simon, P. (2007). *Practical Project Risk Management: The Atom Methodology*: Management Concepts Incorporated.

Hofmann, Mark A. (2008). Public sector faces unique enterprise risk management challenges. *Business Insurance, Volume 42*(Issue 13), 2.

Hofmann, Mark A. (2010). Risk managers struggle with too few staff: Report. http://www.businessinsurance.com/article/20100425/ISSUE01/304259952

Hopkin, P. (2012). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*: Kogan Page, Limited.

Hopkinson, Martin, Close, Paul, Hillson, David, & Ward, Stephen. (2008). *Prioritising Project Risks. A Short Guide to Useful Techniques*: Association for Project Management.

Hulett, David. (2004). Using Quantitative Risk Analysis to Support Strategic Decisions. *Business Risk Management, Volume 19*.

Hulett, David. (2012). What Every Executive Needs to Know about Project Risk Management. http://www.projectrisk.com/white_papers/What_Every_Executive_Needs_to_Know_About_Project_Risk_Management.pdf

Hwang, Min-Shiang, Li, Chun-Ta, Shen, Jau-Ji, & Chu, Yen-Ping. (2004). Challanges in e-government and Security og Information. *Information & Security, Volume 15*(No. 1), 11.

Information & Security. (2004). Editorial: E-government and Security of Information. *Information & Security, Volume 15*(No. 1).

Intaver. (2004). Qualitative and Quantitative Risk Analysis. 3. http://www.intaver.com/Articles/Article_QuantitativeRiskAnalysis.pdf

ISACA. (2009). The RiskIT Framework.

ISO. (2005). ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements.

ISO. (2008). ISO/IEC 27005 Information technology - techniques - Information security risk management.

ISO. (2009). ISO/IEC 31000 Risk management - Principles and guidelines.

Jacobsen, Dag Ingvar. (2003). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. Kristiansand, Norway: Høyskoleforlaget AS.

Jansen, Arild, & Schartum, Dag Wiese. (2008). *Elektronisk forvaltning på norsk. Stalig og kommunal bruk av IKY*. Bergen: Fagbokforlaget.

Joseph, Idolor Eseoghene. (2010). Project Decisions under Uncertainty: Applications to Publicly Financed Project. *European Journal of Economics, Finance and Administrative Sciences, Volume 27*.

Joshi, Ankush, & Tiwari, Haripriya. (2012). Security for E-governance. *Journal of Information and OPerations Management, Volume 3*(Issue 1), 4.

Kappelman, Leon A., McKeeman, Robert, & Zhang, Lixuan. (2006). Early Warning Signs of IT Project Failure: The dominant dozen. *Information Systems Management, 23*(4), 6.

Koh, Lenny, & Simpson, Mike. (2005). Change and uncertainty in SME manufacturing environments using ERP. *Journal of Manufacturing Technology Management, Volume 16*(No. 6), 25.

Kutsch, Elmar. (2008). *Barriers to Project Risk Management. Processes, Techniques and Insights*. Saarbrücken, Germany: Verlag Dr. Müller.

Kvale, Steinar. (2007). *Doing Interviews*: The SAGE Qualitative Research Kit.

Letens, G., Nuffel, L. Van, Heene, A., & Leysen, J. (2008). Towards A Balanced Approach for Risk Identification. *Engineering Management Journal, 20*(3), 7.

Lipshitz, Raanan, & Strauss, Orna. (1997). Coping with Uncertainty: A Naturalistic Decision-Making Analysis. *ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES, Volume 69*(No 2), 14.

McCubbrey, Donald J. (2010). Leveraging with information technology: What is IS risk management. http://cnx.org/content/m35517/1.4/

McNurlin, Barbara Canning, & Sprague, Ralph H. (2009). *Information Systems Management In Practice* (8 ed.). New Jersey: Prentice Hall.

Merna, Tony, & Al-Thani, Faisal. (2008). *Corporate Risk Management*. England: John Wiley & Sons, Ltd.

Misuraca, Gianluca, Alfano, Giuseppe, & Viscusi, Gianluigi. (2011). Interoperability Challenges for ICT-enabled Governance: Toward a pan-European Conceptual Framework. *Journal of Theoretical and Applied Electronic Commerce Research, Volume 6*(Issue 1), 95-111.

Myers, Michael D., & Newman, Michael. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, Volume 17*.

Neimat, Taimour Al. (2005). Why IT Projects Fail. 8.

NIRF. (2005). Helhetlig risikostyring - et integrert rammeverk.

Norsk Standard. (2008). Krav til risikovurderinger.

Northrop Grumman Coroporation. (2007). Risk Management Plan (pp. 13).

Norwegian Ministries. (2012). Digitizing public sector services - Norwegian eGovernment Program.

Novakouski, Marc, & Lewis, Grace A. (2012). Interoperability in the e-Government Context. *Software Engineering Institute*.

Oates, Briony J. (2006). *Researching Information Systems and Computing* University of Teesside, London, England: Sage Publications.

PMBOK. (2008). A Guide To The Project Management Body of Knowledge: Project Management Institute.

PMI. (2009). Practice Standard for Project Risk Management.

Powell, Philip L., & Klein, Jonathan H. (1996). Risk management for information systems development. *Journal of Information Technology, 11*, 10.

PRINCE2. (2013). What is PRINCE2? http://www.prince2.com/what-is-prince2.asp

Project Management Institute. (2009). Practice Standard for Project Risk Management: Project Management Institute.

Remenyi, Dan. (2012). *Stop IT Project Failures through Risk Management*: Taylor & Francis.

Rot, Artur. (2008). IT RIsk Assessment: Quantitative and Qualitative Approach. *Proceddings of the World Congress on Engineering and Computer Science*.

Schneider, Gary P., Lane, Scott, & Burton, Carol M. (2009). Monitoring risk in information technology projects. *Proceedings of the Academy of Information and Management Sciences, Volume 13*(No. 1), 3.

Solli-Sæther, Hans, & Flak, Leif Skiftenes. (2012). Framework for Benefits Realization in e-Government Interoperability Efforts. *9th Scandinavian Workshop on E-Government*, 5.

Sumner, Mary. (2000). Risk factors in enterprise-wide/ERP projects. *Journal of Information Technology, 15*, 10.

Taylor, Hazel, Artman, Edward, & Woelfer, Jill Palzkill. (2012). Information technology project risk managemen: bridging the gap between research and practice. *Journal of Information Technology, 27*, 17.

Tesch, Debbie, Kloppenborg, Timothy J., & Frolick, Mark N. (2007). IT project risk factors: The project management professionals perspective. *Journal of Computer Information Systems*.

The Standish Group. (1994). The CHAOS report: Standish Group.

The Standish Group. (1996). Unfinished Voyages A Follow-Up to The CHAOS Report: The Standish Group.

The Standish Group. (2009). CHAOS Summary 2009: The 10 Laws of CHAOS. http://www.standishgroup.com: Standish Group.

Tiatasin, Krongras. (2012). *IT Risk Management for E-Government Implementation Success.* (Master of Science), Thammasat Business School, Thammasat Business School.

Urquhart, Cathy, Lehmann, Hans, & Myers, Michael D. (2010). Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in informaton systems. *Information Systems Journal, Volume 20*, 24.

Walser, Konrad, Kühn, Andreas, & Riedl, Reinhard. (2009). Risk Management in E-government from the perspective og IT governance. *The Proceedings of the 10th International Digital Government Research Conference*.

Webster, Jane, & Watson, Richard T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, Vol. 26*(No. 2), 11.

Whitmore, Andrew, & Choi, Namjoo. (2010). Reducing the Perceived Risk of E-Government Implementations: The Importance of Risk Communication. *International Journal of Electronic Government Research, Volume 6*(Issue 1), 8.

Wibowo, Arrianto Mukti, & Yuwono, Budi. (2008). Driving Factors, Enablers & Inhibitors of IT Value Delivery & Risk Management in IT Governance.

Williams, Laurie. (2004). Risk Management. http://agile.csc.ncsu.edu/SEMaterials/RiskManagement.pdf

Zhou, Zhitian, & Hu, Congyang. (2008). Study in the E-government Security Risk Management. *IJCSNS International Journal of Computer SIence and Network Security, Volume 8*(No. 5), 6.

8. Appendix 1 – Interview guide

Who	
Organization	
When	
Where	
Duration	
Type of interview	

Introduction

About my master thesis
Part of a master degree in Information Systems
Collaboration with Semicolon-II project
Deadline early June 2013

Recording the interview – get approval
Only for using in this research and for transcribing

Confidentiality – use the name of the organization? Name of your role?

Questions

Time	Topic	Question	Remember
5 min	About the respondent	Could you tell me about yourself	• Name • Education • Experience • Position
2 min	About the organization	Could you tell be about the organization?	• Name • Main competence
2 min	Risk – definition	Could you describe what you consider as risk?	•
20 min	Risk Management	Could you tell me how you work with risk management in your organization?	• Do you follow any framework(s)? • Where in the process do you focus? • What is needed to have more focus on risk? • Challenges

	Interoperability	Could you tell me how you are collaborating with other organizations?	• Benefits • Challenges •
	Risk management + interoperability	How do you work with risk in interoperability projects/efforts	• Split the responsibility • Challenges • Emphasizing? • Ownership
	Wrap-up	• Do you want to add something? • Could you be available for follow-up questions – if necessary?	