# Unveiling Barriers and Enablers of Risk Management in Interoperability Efforts

Pernille Monstad Røberg
Department of Information Systems
University of Agder
PO Box 422, 4604 Kristiansand, Norway
Pernille.Roberg@gmail.com

Leif Skiftenes Flak
Department of Information Systems
University of Agder
PO Box 422, 4604 Kristiansand, Norway
Leif.Flak@uia.no

Per Myrseth
Det Norske Veritas AS
Veritasveien 1
1322 Høvik
Norway
Per.Myrseth@dnvkema.com

## Abstract

*eGovernment efforts are, as general IS efforts, associated with considerable risk. As eGovernment matures and interoperability becomes more ingrained in eGovernment efforts, it will be interesting to explore how the increased complexity affects risk. Still, research on risk management in the context of eGovernment is sparse and our understanding of the phenomenon equally so. This qualitative study investigates risk management in the Norwegian public sector. Based on 11 interviews with experts from nine public organizations, we identified six barriers and eight enablers to risk management in eGovernment settings. Our findings suggest that interoperability has important implications for how risk management is conducted.*

*Key words: Risk management, interoperability, qualitative research, eGovernment.*

## 1. Introduction

IT projects have a long history of failing [1, 2, 3, 4, 5]. According to the much criticized but also frequently cited CHAOS report [4], 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 scholars have studied reasons why IT projects fail. Neimat [6] points to poor planning, unclear goals and objectives and failure to communicate and act as a team. Carlos [7] 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 [8], points to user involvement, good planning and smaller milestones as success criteria for IT projects. Cohn [9] 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. [3] 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 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 [10, 11]. Departments, agencies and other organizations have been asked and advised to report and assess risks in their operations. A growing number of organizations focus on risk and tools like risk matrixes are more commonly used in strategic plans and business plans. Braig et al. [12] suggest that risk management "often is more difficult for public-sector institutions than for private 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 [12].

According to both Duggan [10] and Hofmann [11] 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 organizational procedures, and not be viewed as a separate issue. Other challenges are that there is "no firm and fast definition" and "Everybody thinks there´s some sort of magic checklist" [11]. A third challenge pointed out by Hofmann [11] is that governments can be 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" [13].

Given the challenges of risk management and limited understanding of the phenomenon in the context of eGovernment, this study addresses the following research problem:

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

# 2. Theoretical background

## 2.1. Risk

While the phrase risk has been around for centuries, 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 [14] and PMI [15] risk is an "uncertain event or condition that, if it occurs, has an effect on at least one project objective". PMBOK [14] describes the objectives as scope, cost, quality and schedule. A fifth objective in risk management can be technical constraints [16]. Conrow [16] 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" [17]. As we can see "uncertainty" plays a role within Risk Management.

Uncertainty can be defined as an "unpredictable event that disturbs operation and performance" [18]. Lipshitz and Strauss [19] 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. [20] 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 [21] "risk involves knowing the range of the outcomes; uncertainty involves not knowing the range of outcomes". Also Remenyi [22] supports this by suggesting 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 [22].

## 2.2. Risk management

Risk Management has taken center stage and a review of the history shows that the risk management practice "has been inadequate" [17]. Risks occur in all projects and that is why risk management has become an important part of project management. According to Merna and Al-Thani [23] 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 [23, 24]. Just as risk has many different definitions so has risk management. Merna and Al-Thani [23] 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" [25].

Further, Powell and Klein [25] 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 [26] 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 [23]. 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 [27].

There are many different categories of risk management. According to Chapman [17], organizations face six different classes of risk exposure. These are Financial Risk Management, Operational Risk Management, Technological Risk

Management, Environmental Risk Management, Enterprise Risk Management and Project Risk Management (PRM).

The focus in this study has primarily been on PRM related to public IT projects. PRM can be defined as the process of "conducting risk management planning, identification, analysis, response planning, and monitoring and control on a project" [14]. 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" [14].

## 2.3. Risk management in the public sector

More and more organizations focus on risks and according to both Duggan [10] and Hofmann [11] the public sector faces a challenge when it comes to risk management.

Risks can be found in many areas within the public sector, because the projects have a wide scope and are complex. "E-Governance projects are unique undertakings that involve degree of uncertainty and inherently risky" [28]. According to the same authors, a challenge within eGovernment is that risk management and eGovernment projects are full of risk and uncertainties" [29]. Research focuses on risk factors, but there is little attention to risk assessment frameworks and eGovernment in the literature [28],

According to Tiatasin [30] risks within eGovernance can be found in five areas; IT Infrastructure risk, Economic risk, Legal and regulation risks, Change Management Risk and Performance Risk. Choudhari et al. [28] 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" [28].

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 [31]. According to Bélanger and Carter [31] "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 [32]. Whitmore and Choi [32] suggest that "U.S. citizens prefer a slower pace of expansion".

In order to succeed with eGovernance and reduce the risks needed to communicate with the citizens Whitmore and Choi [32] 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 et al. [33] suggest eight classifications of communication in eGovernment, where one can communicate between and across government, officeholder, citizen and business. Zhou and Hu [34] point to three types of 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 [35] 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. [12] 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:

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

Risk culture is closely related to risk awareness and according to [36] 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 [36].

Risks and issues related to interoperability become more difficult when two or more organizations are collaborating. Potential challenges with interoperability include different risk management cultures or different goals among collaborating organizations. Further, unclear responsibility of risk management is seen as a key challenge [37]. Interoperability has become increasingly significant in the EU in recent years and it is mentioned as an essential prerequisite for eGovernance [38].

## 3. Research approach

The aim of the empirical study was to develop a deeper understanding of the barriers and enablers of risk management in public ICT efforts. In order to get such an understanding, we adopted a qualitative research approach carried out by conducting 11 interviews in 9 organizations. The study was conducted during the spring of 2013.

A grounded theory approach was chosen to allow us to go in depth on risk management and to develop a deeper understanding of barriers for risk management in public ICT efforts. We used grounded theory as an approach of structuring and analyzing the data gathered, rather than a complete method.

The selection of respondents was based on opportunity sampling through the researchers network. Opportunity sampling can also be called convenience sampling and is a part of the larger term "non-probabilistic sampling", which reflects that respondents are chosen based on naturally occurring groups [40]. The aim of the empirical study was to investigate risk management in the Norwegian public ICT effort. Respondents were experts from organizations having experience with risk management in relations to ICT and/or interoperability projects.

We interviewed representatives from eight different government agencies about their experiences with risk management. Further, two representatives from the private sector were interviewed. 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.

Table 1 gives an overview of the respondents of this study and their role. The respondents are given a random number to ensure 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** |
|---|---|---|
| Respondent 1 | Public | Manager |
| Respondent 2 | Public | IT manager |
| Respondent 3 | Public | Project Manager |
| Respondent 4 | Public | IT Manager |
| Respondent 5 | Private | Consultant |
| Respondent 6 | Public | Advisor |
| Respondent 7 | Private | Consultant |
| Respondent 8 | Public | Project Director |
| Respondent 9 | Public | Manager |
| Respondent 10 | Public | IT Manager |
| Respondent 11 | Public | Head of department |

**Table 1. Overview of respondents**

For a grounded theory approach to the data analysis there are three phases related to coding data: open,

axial and selective [40]. Open coding relates to the initial process of labeling the data. It was during this phase that we ended up with a high number of categories. It is important to emphasize that the categories emerging are 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 we 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 was identified, we revisited previously coded data to see if the coding could be improved. This way the emerging theory is related to the empirical data [40].

## 4. Findings

Initially, the findings are presented as categories of enablers and inhibitors of risk management. 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 we had a high number of categories, but as the interviews were completed we revisited the categories several times and got a new view on them. This new view provided useful information and understanding of the relationship between the categories. Several categories were therefore merged.

### 4.1. Process

The use of process, method and framework varied among the respondents. Most of the respondents used one or more frameworks, but 2 respondents did not have a framework for risk management. Three respondents reported that they used ISO 31000 and/or 27001/2 as framework. The remaining 6 respondents were using their own framework and adjusted it to the need within different projects. All respondents were identifying risks, defining risk element, setting probability and consequence and making actions within their project. Ten of the respondents used 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 were differences in how the respondents defined the risk matrix. Some said that green is ok and they do not need to make any actions, other said they needed actions for all identified risks. For some of the respondents, risks that end up in the red area in the matrix meant "stop", for other it meant 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 respondent stated 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. The table below (Table 2) gives an overview of the barriers and enablers from this category

| Barrier | Enabler |
|---|---|
| • Complex framework | • Simple framework<br>• Visualization<br>• Opportunity for prioritization |

**Table 2 - Process Barriers and Enablers**

### 4.2 Management

Management involvement was another topic that several respondents pointed out. Support from top management was seen as a critical success factor. The respondents felt management needed to focus on risk management and demonstrate it to the employees. They felt a need to be measured on risk management just as any other activity they do. In some cases the employees kept 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 management is managing. And this means that they need to understand risk"* (R6).

Six respondents highlighted that one should focus on usefulness when it comes to getting employees committed to risk management. If 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).

Some respondents noted 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).

Other respondents thought there was an important difference between imposing requirements and making risk management a compulsory exercise. If management required that teams 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 3) gives an overview of the barriers and enablers from this category:

| Barrier | Enabler |
|---|---|
| • Lack of top management support | • Demonstrate usefulness<br>• Impose requirements |

**Table 3 - Management Barriers and Enablers**

## 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 rest with 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 was seen as an import aspect of managing risks. If new risk emerged it was important to communicate the changes to the rest of the team and the managers that makes the decisions. This should be a topic on every project meetings. Are there any changes? Is there anything that potentially can harm us? Good communication was viewed as an enabler and something that could 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

Several respondents pointed out that having awareness of risk and how risk can impact the organization and its projects as a key enabler. 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).

Yet 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 we 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 was 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 was also important to be able to get better value from 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 highlighted that it was 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 was 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 did not believe competence to be as important as other respondents. *"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 viewed 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 had 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 was not the only one who had 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 pointed out that a key element within risk methodologies and tools were to harmonize the bits and pieces into a coherent whole. *"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 thought that harmonizing was rather easy and uncomplicated. *"It is not complicated as most risk methodologies are based on the same structure. Its just that they make their own versions"* (R6).

### 4.10. Risk and interoperability

Risk management in relations to interoperability has different perceptions among the respondents. Risk was also managed differently among the respondents when it comes to interoperability projects. The majority of the respondents thought that managing interoperability projects were more complex and challenging than other types of projects.

Respondent 5 thought that interoperability projects were challenging and that it was more important to have control on the risks *"Much more challenging, and the more important to have control on the risks"* (R5). This idea was 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 emphasized that it was more important to have a mutual understanding, agreement and perception of risks when it came 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 thought interoperability projects were complex, much more challenging and time consuming than other projects. *"It is very much one should agree on"* (R9). Further, Respondent 9 pointed 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 was 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).

## 5. Conclusion

This study has investigated challenges of risk management in practice based on Norwegian public ICT efforts. The aim of the study was to answer the following research question:

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

The results show that Risk Management in public ICT efforts can be challenging and complicated. A number of barriers and enablers were identified and categorized.

There is a degree of consistency between our findings and the general literature on risk management. The literature revealed a long list of key success factors, barriers and enablers and some of them were identified in the interviews. However the interviewees also pointed to important issues not found in the literature. Two enablers found in the empirical study but not in the literature are simple frameworks and visualization.

This study shows that lack of framework is not the sole reason for risk management to be challenging. Also lack of support from management offers challenges. As shown in Table 4, this study has revealed several enablers and barriers for risk management in public ICT efforts.

When managing risks in interoperability efforts it is increasingly important to agree on various 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.

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

**Table 4 – Results**

## 6. Implications

This study contributes to research on the topic of risk management in the context of eGovernment, and contributes to increased understanding and knowledge of risk management in practice in public organizations. Our study can create a foundation for further research on the topic of risk management in the public sector. One could do a study in similar organizations to the ones studied and examine the topic in a broader sense, e.g. by examining more respondents from the public sector. Further research is needed to validate and extend our findings and further increase the understanding of risk management in the public sector.

Our results can 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 barriers and enablers presented in this paper 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.

Based on our findings, the following recommendations can be made for organizations adopting or improving their risk management process:

- 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 in interoperability efforts

The following recommendations can be made for 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

## 7. Acknowledgement

This research was in part sponsored by the Semicolon II Project supported by The Research Council of Norway, contract no 201559.

## 8. References

[1] K.De Bakker, A. Boonstra, and H. Wortmann, (2009). Does risk management contribute to IT project success? A meta-analysis of empirical evidence. *International Journal of Project Management*, pp. 493-503.

[2] D.V. Chulkov, and M.S. Desai, (2005). Information Technology Project Failures. Applying the bandit problem to evaluate managerial decision making. *Information Management & Computer Security,* pp. 135-143.

[3] L.A. Kappelman, R. McKeeman, and L. Zhang, (2006). Early Warning Signs of IT Project Failure: The Dominant Dozen. *Information Systems Management*. pp. 31-36.

[4] The Standish Group (1994). The CHAOS Report. pp. 1-8.

[5] The Standish Group (2009). CHAOS summary 2009. The 10 Laws of CHAOS. pp 1-4.

[6] T.A. Neimat (2005). Why IT Projects fail. *The PROJECT PERFECT White Paper Collection*. Pp 1-8.

[7] T. Carlos (2008). Reasons Why Projects Fail.

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

[9] M. Cohn (2006). Agile Estimating and Planning. Pearson Education, Inc. Prentice Hall: USA.

[10] O. Duggan. (2006) Enterprise risk management - the challenge for the public sector. *Accountancy Ireland, Volume 38*. pp 25-27.

[11] M.A. Hofmann (2008). Public sector faces unique enterprise risk management challenges. *Business Insurance, Volume 42*. pp 15-16.

[12] S. Braig, B. Gebre, and A. Sellgren, (2011). Strengthening risk management in the US public sector. pp 1-10.

[13] K. Walser, A. Kühn, and R. Riedl, (2009). Risk Management in E-government from the perspective of IT governance. *The Proceedings of the 10th International Digital Government Research Conference*. pp 315-316.

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

[15] PMI. (2009). Practice Standard for Project Risk Management. Project Management Institute: USA.

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

[17] R.J. Chapman (2011). *Simple Tools and techniques for enterprise risk management*. (Second edition ed.): Wiley Finance: UK.

[18] S.C.L Koh, and M. Simpson, (2005). Change and uncertainty in SME manufacturing environments using ERP. *Journal of Manufacturing Technology Management. pp 629-653*.

[19] R. Lipshitz and O. Strauss, (1997). Coping with Uncertainty: A Naturalistic Decision- Making Analysis. *Organizational behavior and human decision processes. Pp* - 149–163.

[20] I.E. Joseph (2010). Project Decisions under Uncertainty: Applications to Publicly Financed Project. *European Journal of Economics, Finance and Administrative Sciences. Pp 94-109*.

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

[22] D. Remenyi. (2012). *Stop IT Project Failures through Risk Management*: Taylor & Francis: UK.

[23] T. Merna, and F. Al-Thani, (2008). *Corporate Risk Management*. John Wiley & Sons, Ltd: UK.

[24] Northrop Grumman Coroporation, 2007. Risk Management Plan. USA.

[25] P.L. Powell and J.H. Klein (1996). Risk management for information systems development. *Journal of Information Technology*. Pp – 309-319.

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

[27] D. Hulett. (2012). What Every Executive Needs to Know about Project Risk Management.

[28] R.D. Choudhari, D.K. Banwet, and M.P Gupta, (2006). Identifying Risk Factors in for E-governance Projects. Pp 270-277.

[29] R.D. Choudhari, D.K. Banwet, and M.P Gupta, (2005). Risk Profile in E-governance Project. 3rd International Conference on E-Governance. Pp 70-75.

[30] K, Tiatasin. (2012). *IT Risk Management for E-Government Implementation Success*. Thailand.

[31] F. Bélanger and L. Carter. (2008). Trust and risk in e-government adoption. *Journal of Strategic Information Systems*. Pp 165–176.

[32] A. Whitmore and N. Choi. (2010). Reducing the Perceived Risk of E-Government Implementations: The Importance of Risk Communication. *International Journal of Electronic Government Research*. Pp 1-8.

[33] MS Hwang, CT Li, JJ Shen, and YP Chu. (2004). Challenges in e-government and Security of Information. *Information & Security*. Pp 9-20.

[34] Z. Zhou, and C Hu. (2008). Study in the E-government Security Risk Management. *IJCSNS International Journal of Computer Science and Network Security*. Pp 208- 213.

[35] A.M. Wibowo and B. Yuwono (2008). Driving Factors, Enablers & Inhibitors of IT Value Delivery & Risk Management in IT Governance. Pp 1-14.

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

[37] B.D. Adams, S. Waldherr and K. Lee (2007). Interoperable Risk Management in a Joint Interagency Multinational Environment: On behalf of Department of national defence: Canada.

[38] G. Misuraca, G. Alfano, and G. Viscusi. (2011). Interoperability Challenges for ICT-enabled Governance: Toward a pan-European Conceptual Framework. *Journal of Theoretical and Applied Electronic Commerce Research*. Pp 95 -111.

[39] J.W. Creswell. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*: Sage Publications: Los Angeles.

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