Cloud adoption and cyber security in public organizations: an empirical investigation on Norwegian municipalities

TRYGVE VALBØ

SUPERVISOR

Paolo Spagnoletti

University of Agder, 2023

Faculty of Faculty of Social Sciences

Department of Information Systems

PREFACE

This thesis marks the end of my academic journey in cyber security at the University of Agder. The period of being a student here has been enjoyable and enriching in both academic and social aspects. The completion of this extensive, independent project has been an intriguing and challenging process. I have found it to be a pleasant experience in delving into a field that holds my interest and keeps me continuously engaged.

Primarily, I want to express my gratitude to my supervisor, Associate Professor Paolo Spagnoletti. Your guidance has motivated me, introducing interesting perspectives and giving me faith towards my thesis. That, along with your valuable feedback, my overall experience has been truly pleasurable. Additionally, I want to appreciate the enlightening subjects and lectures I have experienced during my years at the University of Agder.

My sincere thanks go to everyone who has been part of this thesis journey. I am grateful to the faculty members for their knowledge sharing, the informants for providing essential empirical data, my peers for insightful discussions, and my family for their consistent support throughout the writing of this thesis.

A heartfelt thank you to all for your contributions to this pivotal moment in my academic path. Your input has been genuinely invaluable.

Abstract

The public sector in Norway, particularly municipalities, is currently transforming through the adoption of cloud solutions. This multiple case study investigates cloud adoption and its security challenges that come along with it. The objective is to identify the security challenges that cloud solutions present and techniques or strategies that can be used to mitigate these security challenges. The Systematic Literature Review (SLR) provided valuable insights into the prevalent challenges and associated mitigation techniques in cloud adoption. The thesis also uses a qualitative approach using Semi-Structured Interviews (SSI) to gather insight into informants' experiences regarding cloud adoption and its security challenges. The study's empirical data is based on interviews with six different Norwegian municipalities, providing a unique and broad perspective. The analysis of the empirical findings, combined with the literature, reveals several security challenges and mitigation techniques in adopting cloud solutions. The security challenges encompass organizational, environmental, legal, and technical aspects of cloud adoption in the municipality. Based on the findings, it is recommended that Norwegian municipalities act on these issues to ensure a more secure transition to cloud solutions.

Kristiansand,

June 2nd, 2023

Table of contents

List of Tables

List of Figures

1. INTRODUCTION

The rapid adaptation of technology has pushed organizations to adapt to new solutions constantly. For every organization and every citizen is dependent on the current technology to communicate efficiently and participate in work processes to maintain access to information. Almost every interaction a user has with an Information and communications technology (ICT) generates data, and we expect these systems to work instantly and at any time.

Since the Eastman Kodak was the first to coin the term of IT-outsourcing, back in 1989, organizations have increasingly turned to outsourcing their Information and Communications Technology (ICT) systems, executing this shift in various stages (Khalfan, 2004, p. 30). With the advent of the world wide web in the 1990s, there was a growing necessity for efficient management of data, information, and knowledge (Hamlen & Thuraisingham, 2013, p. 1). With the entrance of the internet a new way of ICT-outsourcing emerged which provided flexible and cost saving services. This is formerly known as cloud computing. One definition of cloud computing is:

“Cloud Computing delivers computing services—data storage, computation and networking—to users at the time, to the location and in the quantity they wish to consume, with costs based only on the resources used. Users simply procure from providers the “amount of computing” they want without needing to invest in computing infrastructure.”

(Kushida, Murray, & Zysman, 2011).

The emergence and growing popularity of cloud solutions over the past 20 years have significantly transformed the ICT-landscape. Cloud computing offers a more flexible and scalable solution, allowing organizations to use ICT-resources as services over the internet on a pay-per-use basis. This approach has introduced a new level of agility and cost-effectiveness in managing ICT requirements (Mvelase, Dlodlo, Williams, & Adigun, 2011, p.1).

Organizations in the public sector varies in terms of requirements, risk orientations, funding, and resources available. However, they have one thing in common, and that is selecting ICT solutions that are both suitable and economical for their specific needs (KMD, 2015, p. 2). The diversity of Norwegian municipalities provides a compelling study in this regard. Aspects such as the size, function, requirements, and resources are significant. They are significantly different in terms of size, function, requirements, and resources. Municipalities span the spectrum from large metropolitan areas such as Oslo and Bergen, to medium-sized towns like Kristiansand and Ålesund, all the way down to small communities of around 2000 inhabitants.

Some municipalities have decided to collaborate with several municipalities and form an inter-municipal organization that function as a common platform that serve ICT-service and acquisition. Example of this is Agder IKT or ROR-IKT. These collaborations foster mutual support and resource sharing, providing smaller municipalities with access to larger, shared ICT-systems.

The Norwegian government, published in 2015 a cloud strategy for public organization, mentioning that. “Cloud solutions must be evaluated in line with other solutions when one is faced with a larger one changes or restructuring of the ICT-system or operation:” [Translated] (KMD, 2015, p. 25). This is as close the Norwegian government has come to a “cloud first” strategy. Eight years later Norwegian municipalities has grown dependent on these cloud solutions.

Cloud adoption will expand the digital supply chain with a complex system. More significant risks lead to dependency and vulnerability in the supply chain, which poses an increased attack surface for cyber-attacks (NSM, 2020, p. 3). The Norwegian National Security Authority (NSM) has expressed some concern about this development. They say that "We are concerned about the overall and national dependence on foreign cloud providers" (NSM, 2020). This implies that there is a legal risk in that Norwegian services are delivered from abroad. There is a concentrated risk in that a small number of suppliers carry these functions.

In the landscape of cloud computing most significant vendors are Microsoft, Amazon, and Google. This means that the processing and storage of data outside of Norway are quite widespread for municipalities. Many Norwegian governmental organizations do not necessarily have sufficient control over where their data is located at any given time.

This presents challenges considering that many Norwegian societal functions depend on these suppliers (Seip, 2020).

In 2020, the European Court of Justice ruled the so-called Schrems II Decision[1], which problematized the legal framework for transfers of personal data to a third country which is USA. The decision has set a new standard for transferring personal data to third countries. This is a problem that many European organizations must deal with today. Municipalities that adopt to cloud solutions face the same issues (Digdir, 2020).

NSM points out that public agencies should have several managerial principles in place if it chooses to use cloud solutions. The recommendations are to have good ordering skills, to have a good overview and control over the entire life cycle, to have good risk assessments to be able to make the right decision, to be able to make the right and reasonable demands on the ICT-service and the supplier and to make the right decision at the right level (NSM, 2020).

Many municipalities in Norway lack the competence to make such decisions (Steen, 2022). Considering that municipalities process sensitive information from users, such as health information, address, phone number, social security number, and many other data that is considered sensitive. This makes the impact of data disclosure even higher. Based on all NSM's recommendations, does Norway's municipalities have enough resources to ensure security is safeguarded when the adoption of cloud solutions takes place so quickly?

1.1 Motivation

Number of incidents of supply chain attacks is increasing, and it is a significant threat (NSM, 2020, p. 3) It is important to protect municipal systems and mitigate the likelihood of cyber incidents, which can have critical consequences if not addressed. These supply chains extend internationally, implying that the Norwegian systems are no longer strictly domestic, but rather operate within a Volatile, Uncertain, Complex, and Ambiguous (VUCA) environment, primarily due to their international extension (Bennett & Lemoine, 2014). Norwegian municipalities must be prepared to manage

[1] Schrems II Decision is that the EU court deemed the Privacy Shield between EU and USA invalid.

potential risks, particularly considering the prevailing threat environment across Europe (NSM, 2023).

For public organization it is important to know how what the common pitfalls that can happen when they adopt to cloud solutions. Hence, this thesis sets out to identify and analyze the challenges. Given the limited research in the field cloud adoption within the context of public organization, there is an opportunity to contribute to this field of study. It is particularly motivating to spread awareness of the critical need for prioritizing cybersecurity as municipalities navigate their transition to cloud solutions. By so doing, this thesis can contribute the understanding and implementation of security measures in such settings, ensuring safer and more efficient use of cloud technologies.

1.2 Research Questions

In the effort to narrow down the effort scope of this thesis, I have formulated research questions. The role of these research question is to guide me through this study, reducing the possibility of complications during my research process (Creswell, 2014). The research question(s) explore the context of Norwegian public organizations and the phenomenon of cyber security challenges that occur during cloud adoption as well as how to mitigate them. The main research question is then further dissected into two more focused questions.

Main Research Question:

“*What are the cybersecurity challenges experienced by public organizations in the adoption of cloud solutions, and how can they address these concerns?”*

Further, to break down the research question to first focus on the challenges public organizations experience:

“What are the security issues that public organizations experience when adopting cloud solutions?”

Secondly the last research question addresses how public organizations deal with the challenges:

“How can public organizations ensure cyber security when adopting cloud solutions?”

To be able to answer my research question and achieve a deep understanding of the problem, a literature review as well as a qualitative research method will be applied to my problem domain.

1.3 Thesis Structure

The thesis will have six chapters. Chapter 2 will consist of exploring literature that is relevant to the topic. This section will also contain a literature discussion, such as a Systematic Literature Review (SLR).

Chapter 3 is about the methodology used in the thesis, divided into different parts such as literature review, research strategy, research approach, and design. This section concerns our research methodologies, data collection and analysis.

Chapter 4 is a summary of the analyzed data that was collected during the interviews.

Chapter 5 includes discussions of what was in the related literature section and our findings. Further, the data is then discussed. It will contain a discussion of the results. The limitation and proposes the way ahead for further research will also be addressed in this chapter.

Chapter 6 contains a conclusion of the entire thesis. Reading this chapter will summarize the whole thesis.

2 BACKGROUND AND RELATED WORK

In this section, I will present the findings from the literature review, which consist of exploratory research delving into the topics of security issues of first outsourcing ICT-systems and cloud solutions. The findings from my literature review have been organized in a table where it lists the security issues and the mitigation techniques that mitigate the security issue.

Table 1 Literature review findings

Theme	Security Issue	Description	Mitigation Technique(s)
Organizational	Due diligence	Traditional outsourcing and cloud sourcing demand due diligence to circumvent pitfalls, including the potential loss of data control (Pai & Basu, 2007, p. 29). These tasks become increasingly challenging with limited access to vendors' services, system complexity, and associated costs (Bachlechner et al., 2013, p. 44; Kshetri, 2013, p. 379). This creates transparency issues that arise from uncertainties surrounding whether processed data has been adequately deleted by vendors or sub-vendors, thereby complicating the selection and audit processes (Pearson & Benameur, 2010, p. 694; Svärd, 2018 p. 136).	Mitigation efforts should include tightly due diligence processes, demanding more from the vendor such as vendor documentation, intrusion detection tests, and security measure authentication protocols (Pai & Basu, 2007, p. 31). By performing continuous monitoring of Service Level Agreements (SLAs) can ensure that the agreements are being complied with (Wulf, et al., 2019, p. 260). Involvement in collaborative initiatives like the UK G-Cloud digital marketplace and The American Institute of Certified Public Accountants (AICPA) can further give “free” assessment of the cloud solutions more

Theme	Security Issue	Description	Mitigation Technique(s)
			efficiently due to more resources available (Ksheri, 2013, p. 379; KMD, 2015, p. 31).
	Lack of user awareness	The human factors are often leading cause of cyber security incident, especially with the increasing use of cloud solutions (NSM, 2020, p. 25). Implementing comprehensive security training programs can help mitigate these risks, although this becomes more complex in IT-outsourcing arrangements (Wulf et al., 2019, p. 263; Bachlechner et al., 2013, p. 40). This complexity is exacerbated by vendors who may not enforce security policies consistently, creating potential security gaps (Khalfan, 2004, p. 38; Dhillon, Seyd & Soares, 2017, p. 454).	To mitigate the lack of user awareness, effective management of human resources, including targeted security education and awareness campaigns, is key (Nassimbeni, Sator & Dus, 2012, p. 414). Clear policies should be developed and implemented, complemented by comprehensive staff training on security issues (Khalfan, 2004, p. 38; Bachlechner et al., 2013, p. 47).
	Management's involvement roles and responsibility	The success of IT projects, especially cloud adoption, hinges significantly on management support, with a lack thereof leading to potential project derailment (Nakatsu & Iacovu, 2009, p. 58; Tafti, 2005, p. 554). The degree of managerial involvement can influence project outcomes, as can their qualifications and knowledge, particularly when inadequate expertise may give too much control to vendors (Nakatsu & Iacovu, 2009, p. 62).	To counter these challenges, fostering communication between IT managers and business leaders is key, a solution proposed by Hansen, Kraemmergaard & Mathiassen, through a model focusing on mutual understanding and collaboration (Hansen et al., 2011, p. 183).
Legal Aspects	Legal Issues	Offshore outsourcing and cloud solutions can lead to legal, financial, and communication challenges, especially when data crosses jurisdictional boundaries (Ghaffar, 2020; Nakatsu & Iacovou, 2009 p. 64; Pai & Basu,	Mitigation strategies include governmental efforts to simplify and unify laws, revise archival practices, harmonize supervisory requirements, and

Theme	Security Issue	Description	Mitigation Technique(s)
		2007; Nassimbeni, Sator & Dus, 2012, p. 408).	align with EU efforts for standardized cloud services criteria. (Scholtz, Govender & Gomez, 2016, p. 11).
Environmental issues	Trust	Outsourcing entails significant trust between the vendor and client, with the security of data resting largely on the vendor's abilities (Dhillon et al., 2016, p. 457; Xiao & Xiao, 2012, p. 844). However, this reliance can introduce risks, especially when trust boundaries are blurred in public or hybrid cloud setups and within vendor supply chains (Pearson & Benameur, 2010, p.965).	Thus, to ensure successful cloud adoption, it's crucial to establish trust through extensive attention to security, data control, and vendor management (Ali & Osmanaj, 2020, p. 17; Pearson & Benameur, 2010, p. 693).
	Losing Control of the Supply Chain	Using cloud providers often leads to extended supply chains, reducing direct control over data storage and processing (Pearson & Benmaeur, 2010; Hamlen & Thuraisingham, 2012, p. 2; Xiao & Xiao, 2012, p. 884). This scenario can challenge data confidentiality and integrity, as it becomes difficult to manage the geographical and organizational boundaries associated with varying cultures, laws, and languages (Nakatsu & Iacovou, 2009, p. 59; Wulf et al., 2019, p. 261). As such, clients become reliant on trust-based agreements like Service Level Agreements (SLAs) to safeguard their data, while facing potential security risks due to the Losing Control of the Supply Chain (Pearson & Benameur, 2010, p. 697).	The mitigation strategies to regain control of the supply chain include establishing well-defined Service Level Agreements (SLAs) and contracts with clear responsibility definitions. Further, they should closely monitor, and regularly revising these agreements (Wulf, et al., 2019, p. 260). Lastly, making concerted efforts to collaborate on initiatives (Kshetri, 2013, p. 379; KMD, 2015, p. 31).

Theme	Security Issue	Description	Mitigation Technique(s)
	Constrained Market Competition	In the context of ICT outsourcing, excessive dependence on cloud providers can result in a power imbalance (Bhatti, Mubarak & Nagalingam, 2021, p. 276; Nassimbeni et al., 2012, p. 407). This challenge is heightened by the potential dominance of a single vendor, which can reduce Service Level Agreements (SLAs) fulfillment and foster unhealthy vendor dependence (Seip, 2020, p. 69; Almutairi & Riddle, 2018, p.45; Ghaffar, 2020, p. 9).	The clients should push vendors to abide by the requirements requested. This will nurture a more diverse vendor market. Thereby enhancing overall service quality and the implementation of robust security measures. (Kshetri, 2013, p. 381)
	Governmental governance with strategies and frameworks	Concerns exist about the absence of approved cloud standards and a lack of clear cloud adoption strategies (Scholtz et al., 2016). Outdated or inappropriate governmental frameworks and guidelines hinder cloud adoption and puts it at a risk (KMD, 2015, p. 27).	Governments need to provide updated, clear, and comprehensive strategies, frameworks, standards, and guidelines for cloud adoption (KMD, 2015, p. 16.)
Technical issues	Availability	Availability and disruptions may arise from different sources, such as technical issues, cyberattacks, natural disasters, software updates, configuration errors, or human errors (Scholtz, et al., 2016, p. 4; p. 58; Nakatsu & Iacovou, 2009, p. 64; Ghaffar, 2020; Xiao & Xiao, 2012, p. 850; Wulf, et al., 2019; Kajiyama, et al., 2017, p. 637; Bhatti, et al., 2021, p. 227). Such disruptions can make an organization vulnerable if their systems or data become unavailable.	Commonly, data redundancy and diversification are employed, often through backups to mitigate availability issues (Hamlen & Thuraisngham, 2013, p. 3; KMD, 2015, p. 11; Kyriakou, Euripides & Paraskevi, 2020, p. 249; Pearson & Benameur, 2010, p.694).
	Confidentiality	Concerns around confidentiality revolve around vendors' ability to protect confidential information (Pai & Basu, 2007, p. 41). Other concerns revolve around risks associated with data transit in the supply chain, the generation	Additionally, to technical mitigation, it is advised to have comprehensive non-disclosure agreements, Service Level Agreements (SLAs), and

Theme	Security Issue	Description	Mitigation Technique(s)
		of potentially confidential metadata, and unauthorized access to cloud solutions (Hamlen & Thuraisingham, 2013, p. 3; Almutairi & Riddle, 2018, p. 45; Wulf, et al., 2019, p. 260). Furthermore, the legal right of governments to access data presents an additional challenge (KMD, 2015, p. 22; Wulf, et al., 2019, p. 260)..	explicit contract terms. These documents can detail important matters such as authentication and user management strategies (Almutairi & Riddle, 2018, p. 45; Ali & Osmanaj, 2020, p. 10).
	Authentication and user management	Unauthorized access, alteration, and disclosure of assets in cloud solutions often stem from inadequate identity management and password confidentiality (Khidzir, Arshad, and Mohamed, 2010, p. 197; KMD, 2015, p. 15; Pai & Basu, 2007, p. 31). Outsourcing systems also introduce the risk of untrusted individuals accessing the solution (Hamlen & Thuraisingham, 2012, p.1). Internal authorization, such as weak authentication practices or non-compliance issues, can also create vulnerabilities, particularly as cloud solutions become more integrated, making the impact of such issues greater (Khidzdir, Mohammed & Arshad, 2010, p. 198; Bachlechner, et al., 2014, p. 56).	For internal authentication issues, it is important that security measures and policies do not become disruptive when enforced (Bachlechner, et al., 2014, p. 56). Externally, clients should perform due diligence by determining whether the service provider offers sufficient customer identity authentication (Pai & Basu, 2007, p. 32). Clients should also ensure an appropriate level of access for the outsourcing vendor, allowing them to effectively fulfill their responsibilities without compromising security (Dhillon, et al., 2017, p. 457).

Theme	Security Issue	Description	Mitigation Technique(s)
	Multi-tenancy	Shared infrastructure in cloud services is where multiple clients' data is stored and processed on the same physical hardware (Xiao & Xiao, 2012, p. 844). This introduces risk by the absence of physical boundaries between different clients' data. This can potentially expose data to unauthorized users. Misconfigurations could inadvertently create access points, allowing unintended access or even privilege escalation (Pearson & Benameur, 2010, p. 696; Wulf, et al., 2019, p. 260; Ghaffar, 2020, p. 8).	Mitigation of multi-tenancy issues are primary getting control over the data lifecycle (Pearson & Benameur, 2010, p. 695). It can be done by implementing robust protective measures and strict oversight. Ensuring data segregation through advanced security features like encryption and strict access controls (Xiao & Xiao, 2012, p. 853).
	Vendor Lock-in	Proprietary standards for data storage often hinders data portability. This can lead to complication in data migration to other solutions (Ghaffar, 2020, p. 9; KMD, 2015, p. 18; Dhillon, et al., 2016, p. 456; Seip, 2020, p. 40). This situation can create a "lock-in" effect, where the cost of exiting the arrangement becomes high, potentially forcing organizations to stick with a vendor's services despite contract violations or subpar service (Ghaffar, 2020, p. 9). This lock-in can introduce various threats, including jeopardizing business continuity, losing cost control, and reduced system customization flexibility (Kajiyama, et al., 2017, p.651).	The recommended mitigation strategy is to establish short-term, annually renewable contracts. This approach allows for flexibility and encourages a more dynamic relationship between the client- vendor, helping to avoid the risk of vendor lock-in of a given cloud solution (Wulf, et al., 2019, p. 262).

2.1 Addressing Security Concerns in Cloud Sourcing: Challenges and Strategies

Despite the rapid adoption of cloud solutions, there are several issues that arise when ICT-systems are outsourced, particularly when it is a cloud solution. Although, it is difficult to provide a complete list of cloud adoption security issues due to several reasons (For example technological changes, The complexity of the IS system and deployment models). In lieu, the security issues can be classified into some broad categories which are Organizational, Technical, Legal, and Environmental.

2.1.1 Organizational issues

Organizational challenges encompass issues that originate from within the organization itself. Since these issues are internal, solutions or mitigation techniques are typically straightforward to implement and effective, as they directly address the root cause of the problem.

2.1.1.1 Due Diligence

Traditional outsourcing requires careful due diligence and legal planning to circumvent common pitfalls, a need that is even more present in cloud sourcing (Pai & Basu, 2007, p. 29). Losing Control Over the Supply Chain, often indicating difficulties in or lack of performing due diligence, can quickly transpire, particularly concerning data whereabouts and processing (Wulf, Strahringer & Westner, 2019). Given that data is held by the cloud provider, continuous audit and control pose significant challenges for the client in an outsourcing arrangement (Tafti, 2005, p. 553; KMD, 2015, p. 17).

To mitigate these risks, additional measures, including thorough documentation of the vendors, intrusion detection tests, documentation of security measures, and authentication and verification protocols, should be assessed (Pai & Basu, 2007, p. 31). However, obtaining such documentation is crucial to meaningful due diligence, yet the restricted access to vendors' services can create obstacles. This difficulty is further exacerbated when dealing with vendors that use sub-vendors or public cloud services (Bachlechner, Thalmann & Maier, 2013, p. 40; Kshetri, 2013, p. 379).

The complexity of the system proportionally impacts the cost of performing due diligence (Bachlechner et al., 2013, p. 44). A significant transparency issue also arises, obscuring whether the vendor or sub-vendor has effectively deleted data post-processing (Pearson & Benameur, 2010, p. 694; Svärd, 2018 p. 136).

Gaining control over the data supply chain entails continuous monitoring of Service Level Agreement (SLA) fulfillment, ensuring the service provider enforces the necessary protective security measures (Wulf, et al., 2019, p. 260). Given the extensive resources this process demands, literature recommends collaborative initiatives such as UK G-Cloud digital marketplace and The American Institute of Certified Public Accountants (AICPA). which is an organization that carries out comprehensive due diligence on cloud systems, providing approval or recommendations to organizations (Ksheri, 2013, p. 379; KMD, 2015, p. 31).

While organizations can utilize standards (Ksheri, 2013, p. 379; KMD, 2015, p. 29), these should be used with caution. Practical cases and academic literature have pointed out that such standards can be counterproductive, offering a false sense of security (Ksheri, 2013, p. 379).

2.1.1.2 Lack of user awareness

The human factor is often considered to be one of the primary determinants in cyber security (Bachlechner et al., 2013, p. 46). As organizations increasingly adopt cloud solutions, they confront the necessity of maintaining attention over this issue (NSM, 2020, p. 25). A mistake by an employee can inadvertently compromise the security, which can lead to dire consequences especially when handling sensitive data.

In general, implementing security awareness training programs emerges as a promising countermeasure for compliance issues, designed to mitigate the possibility of employee errors. However, performing such training is not without its complications. The employees that either store or process data for the cloud solution, must acquire the proper knowledge spanning several domains such as security, data privacy, and risk management (Wulf et al., 2019, p. 263; Bachlechner et al., 2013, p. 40).

Yet, the necessity of training does not stop at the client; vendors are equally responsible for equipping their staff with proper awareness towards security and compliance. The task of achieving and maintaining awareness may be challenging within an organization itself. The complexity multiplies in complex IT-outsourcing arrangements, which cloud solutions usually are (Bachlechner et al., 2013, p. 40).

A further problem arises when utilizing vendors. There is an increasing risk that policies applied within the client might not receive the same degree of enforcement or may not exhibit equivalent strength by the vendors(s) (Khalfan, 2004, p. 38; Dhillon, Seyd & Soares, 2017, p. 454). This issue can lead to a potential gap in security measures, adding another layer of intricacy to the cyber security of the solution.

To mitigate the lack of user awareness, managing human resources effectively have proven to be effective countermeasure (Bachlechner et al., 2013, p. 47). More specifically the security management should address the end-user security in form of awareness, and education. Policies must be developed and implemented clearly to the users (Khalfan, 2004, p. 38).
Thorough planning of staff training regarding security issues (Nassimbeni et al., 2012, p. 414).

2.1.1.3 Management's involvement roles and responsibility

The success of IT-projects, those related to cloud adoption, is heavily dependent on managements' support. A lack of support from management can lead to consequences for the project, making it an uphill battle to stay on track and risking resources being pulled (Nakatsu & Iacovu, 2009, p. 58; Tafti, 2005, p. 554). Tafti (2005) identified that the scale of a project can influence the level of managerial involvement. High-profile projects may make top managers take control of key decisions, potentially marginalizing critical personnel such as the CIO and VP of information systems. Leaving them out of important decisions (Tafti, 2005, p. 554).

This managerial involvement is critical for ensuring resources are in place as well as it is a critical role in fostering collaboration across various organizational groups (Nakatsu & Iacovu, 2009, p. 62; Svärd, 2018). The decision-making process of acquiring cloud solutions usually involves top-position people such as managers and politicians

(Polyviou & Pouloudi, s. 2093). With the lack of knowledge of cloud computing, the willingness to adapt drops (Polyviou & Pouloudi, p. 2092; Nakatsu & Iacovu, 2009, p. 62). If the management lacks expertise, vendors may dominate the cloud adoption process (Nakatsu & Iacovu, 2009, p. 62).

Given these challenges, a potential solution of such issues is to improve the communication, for both parties i.e., IT manager and business leader. A model proposed by Hansen, Kraemmergaard & Mathiassen (2011) was initially to facilitate rapid adaptation in digital transformation. This model focused on intervention on both parties to get both to understand each other's viewpoint. The insights gathered from the model highlight four critical steps to foster mutual understanding between two parties: Engage IS and business leaders, address perceived digitization challenges, jointly explore digitalization options, and address different views on digital transformation (Hansen et al., 2011, p. 183).

2.1.2 Legal issues

Legal challenges, or jurisdictional implications present significant barriers to organizations and constitute one of the most complex aspects of cloud adoption. These issues are convoluted, as they apply across diverse jurisdictional zones, adding layers of complexity. While this thesis will not delve into the specifics of all laws and regulations due to its scope, it will highlight the primary issues and their corresponding mitigation strategies.

2.1.2.1 Legal Issues

As Nakatsu & Iacovou (2009) stated that; Offshore outsourcing often “involves risk of a dispute due to different laws, currency, business, and accounting practices, failure of communication lines and travel, political risk, etc.” (Nakatsu & Iacovou, 2009, p. 64). When it comes to challenges of utilizing cloud solutions or outsourcing for that matter, is the movement of data outside from organizational boundaries. This triggers issues related to laws and regulations. The problem becomes more apparent when the service provider is placed in another country than the client (Ghaffar, 2020; Nakatsu & Iacovou, 2009 p. 64; Pai & Basu, 2007; Nassimbeni et al., 2012, p. 408). The Schrems II case and the safe harbor dispute and EU-US privacy shield have led organizations in Europe to question whether other foreign authorities have access to data due to different laws and jurisdictions, which is concerning for the confidentiality of the data (Dhillon et al., 2016, p. 456). In Norway there are two important laws that affect municipalities on where the data must be stored: the Bookkeeping Act and the Archival in addition to the Security Act (KMD, 2015, p. 19). It is apparent that to adapt to cloud solutions, it is a lack of standards, frameworks, and regulatory requirements for organizations to follow (Scholtz, Govender & Gomez, 2016, p. 11).

Hence, the need for clear and unified laws and framework is needed. Currently there are initiatives in motion at governmental level to counteract the complexity of laws. Firstly, the Norwegian laws should be open for revisions, most importantly consider the need for amendments to allow public bodies to use cloud services with servers that are located outside of Norway for archival purposes. Secondly, extend the number of countries the archival and bookkeeping data can be stored in. Further, the government should make efforts harmonizing supervisory practices, so municipalities do not get conflicting requirements issued by several instances. Finally, to engage in the EU's efforts towards setting unified criteria, including standards and certification schemes, for cloud services. (KMD, 2015, p. 5).

2.1.3 Environmental issues

This theme, also referred to as environmental issues, concentrates on dilemmas that lie outside the organization's boundary. Although the vendor-client relationship naturally is in the focus, other factors such as government and associations come into play in the environmental issues.

2.1.3.1 Trust

Outsourcing the organization's system involves laying a significant amount of trust between the vendor and client. For instance, the organization that outsources must trust the vendor to apply appropriate security controls (Dhillon et al., 2016, p. 457; Xiao &

Xiao, 2012, p. 844). The tendering process of evaluating vendors typically is guided by specific criteria set by the client, based on the request and responses the vendor is announcing (Almutairi & Riddle, 2018, p. 43).

However, relying on trust to a vendor can have implications. If a vendor cannot be trusted to protect the data, the risk of cloud sourcing could outweigh its potential benefits (Pau & Basu, 2007, p. 41). Moreover, the lack of trust can lead to poor quality and performance (Dhillon et al., 2016, p. 458).

In traditional setups, organizations can define their trust boundaries within their organization which they physically can have control over. But, when considering public or hybrid cloud solutions, these boundaries become blurred, complicating the dynamic of trust and control (Pearson & Benameur, 2010, p.965).

Trust issues extend to the supply chain as well. Trusting a vendor also means trusting their sub-vendors, which introduces an additional layer of complexity. How can a client ensure that trust is maintained throughout the supply chain (Pearson & Benameur, 2010, p. 965)?

Therefore, building trust- both in terms of customer and vendor privacy - is essential for successful cloud adoption (Ali & Osmanaj, 2020, p. 17; Pearson & Benameur, 2010, p. 693). Trust in the cloud adoption process is a multifaceted issue, demanding careful attention to security, data control and vendor management.

2.1.3.2 Losing Control of the Supply Chain

Utilizing cloud service providers can result in complex supply chains, potentially impairing the control over data storage and processing (Pearson & Benmaeur, 2010; Hamlen & Thuraisingham, 2012, p. 2; Xiao & Xiao, 2012, p. 884). This, in turn, implies that vendors cannot wholly ensure confidentiality and integrity of the data, as they may not be under the supervision of trustworthy entities (Almutairi & Riddle, 2018; Xiao & Xiao, 2012).

Due to geographical differences and organizational boundaries, maintaining control over the data storage and processing, as well as employee supervision can become challenging. This loss of control may arise due to diverse cultural contexts, legal systems, and languages (Nakatsu & Iacovou, 2009, p. 59; Wulf et al., 2019, p. 261). These challenges often increase as the distance from the organization increases (Pai & Basu, 2007, p. 29).

The loss of data control can expose the company to attacks from adversaries aiming to exploit this weakness (Xiao & Xiao, 2012, p. 847). As a result, customers may find themselves in a weakened position to enforce technical safeguards against unauthorized data access or misuse. Consequently, security becomes increasingly reliant on trust-based contracts, such as SLAs (Pearson & Benameur, 2010, p. 697).

The strategies to regain control of the supply chain would mirror those mentioned in the chapter about Due Diligence. These involve establishing well-defined SLAs and contracts with clearly articulated responsibilities, closely monitoring, and making regular revisions (Wulf, et al., 2019, p. 260), and participating in collaborative initiatives (Kshetri, 2013, p. 379; KMD, 2015, p. 31).

2.1.3.3 Constrained Market Competition

In the realm of ICT-systems outsourcing, an inadvertent dependency on cloud providers is a frequent consequence, often creating an imbalance of power that can be disadvantageous for the client (Bhatti, Mubarak & Nagalingam, 2021, p. 276; Nassimbeni et al., 2012, p. 407). The circumstances can be further complicated when the market is dominated by a single vendor, creating a restrictive and even monopolistic environment.

Such dynamics can reduce the likelihood of Service Level Agreements (SLAs) being fulfilled, owing to a lack of compelling incentives to meet requirements set by the client (Seip, 2020, p. 69). Take Google's service agreements as an example; they state that the company offers no warranty nor takes responsibility for damages resulting from a potential failure to protect privacy and security (Kshetri, 2013, p. 380).

Data confidentiality should be considered a paramount aspect for both the vendor and client. A reliance on vendors may reduce the technical competencies within the client organization, thereby nurturing an unhealthy dependence and potentially giving rise to a form of vendor lock-in. This also leads to ambiguities regarding who is responsible for security (Almutairi & Riddle, 2018, p.45; Ghaffar, 2020, p. 9).

As customer requests are received by vendors, adapting to their clients' constantly evolving security and compliance requirements becomes challenging. Consequently, the financial incentives to make such adjustments are not present. The limited availability of vendor options, coupled with no financial incentives to do the measures, makes it challenging for clients to find a service that provides satisfactory security measures (Bachlechner, et al., 2013, p. 40).

Clients of cloud solutions are increasingly exerting collective pressure on vendors to comply with their specific requirements. This can be done by having a clear SLA or contract with requirements. This approach helps mitigate the power dynamic issue, as clients can opt not to engage with vendors that fail to meet their demands, instead of reluctantly purchasing unsatisfactory services (Kshetri, 2013, p. 381). Thus, this will mitigate many of the other issues that are discussed in this chapter as the requirements force the providers to improve.

Contracts and SLAs are essential tools that clearly delineate the responsibilities of both vendors and clients, providing a legally binding documentation of their respective obligations. They are important to assure effective outsourcing agreements (Pai & Basu, 2007, p. 44; Khalfan, 2004, p. 39). SLAs are employed to outline the anticipated service quality, and the objectives to be achieved, as well as address other matters such as legal and financial concerns (Abdullah & Quintero, 2019, p. 602; Wulf, et al., 2019). SLAs relieves the issue of laying too much trust in the vendors as it can be seen as a legal document (Kshetri, 2013, p. 381).

2.1.3.4 Governmental governance and control

When it comes to guidance and control, the government can play a role in influencing organizational cloud adoption through different manners. The most prominent is guidelines, frameworks, strategies, and laws. However, it is worth mentioning that the legal aspects are addressed in its own chapter.

According to a comprehensive organizational study performed by Scholtz et al. (2016), 65% of its informants voiced their concerns about the availability of approved cloud standards, while 75% were worried about the lack of a strategy or guidelines for cloud adoption. (Scholtz et al., 2016). These findings underscore the role of the government in providing frameworks. In the Norwegian context, governmental bodies such as NSM and KMD have provided several guidelines and strategies, including the most prominent: "Cloud Computing Strategy for Norway.".

However, a study by Seip (2020) reveals that none of the respondents had a sourcing strategy, which is a crucial consideration for reducing risk in cloud solution adoption. This underscores the importance of addressing this aspect in governmental initiatives (Seip, 2020, p. 11).

It is important to acknowledge that frameworks, guidelines, and standards can sometimes become outdated and may not be grounded in the current environment (KMD, 2015, p. 22). As discussed earlier, frameworks and standards that are not suitable cloud adoption can create a false sense of security (Scholtz, et al., 2016, p. 11). If an unappropriated framework is used, it can compromise the security of cloud solutions. For instance, standardized frameworks such as the Government Standard Terms and Conditions (SSA) are deemed to not be well-suited for cloud solutions (KMD, 2015, p. 27). This highlights the need for clear and suitable frameworks, standards, and strategies for cloud adoption (KMD, 2015, p. 16).

2.1.4 Technical issues

2.1.4.1 Availability

Unsurprisingly, as a cornerstone of information security, the availability of their systems is a vital concern for organizations, when it comes to cloud solutions. The organization can become vulnerable if their systems or data become unavailable at a given time. For example, frequent issues such as lost internet connection or inadequate infrastructure can disrupt their operations (Scholtz, et al., 2016, p. 4; p. 58; Nakatsu & Iacovou, 2009, p. 64).

Furthermore, disruptions are not only limited to technical difficulties. Malicious actions such as cyber-attacks pose a significant threat (Ghaffar, 2020; Xiao & Xiao, 2012, p. 850; Wulf, et al., 2019). Natural disasters, including storms and fires, are other potential sources of disruption (Kajiyama, et al., 2017, p. 637). Additionally, technical hiccups such as software updates and configuration errors (Bhatti, et al., 2021, p. 227), and human errors driven by cultural or language barriers can create to downtime or disturbance of the system (Nakatsu & Iacovou, 2009, p. 58).

Organizations might enforce countermeasures to mitigate availability of cloud solutions, the most common mitigation technique is to have redundancy or diversify the data, which is typically done with backups (Hamlen & Thuraisngham, 2013, p. 3; KMD, 2015, p. 11; Kyriakou, Euripides & Paraskevi, 2020, p. 249; Pearson & Benameur, 2010 , p.694). These countermeasures might be prohibitively expensive (Scholtz et al., 2016, p. 4). Moreover, given the unpredictability of some events, it is challenging to ensure a complete, 100% safeguard against all potential disruptions (Kajiyama, et al., 2017, p. 637).

2.1.4.2 Confidentiality

Confidentiality serves as one of the pillars in information security along with availability, and it emerges as a prominent issue when municipalities utilize cloud solutions (Kyriakou, et al., 2020, p. 245). The concept of confidentiality bears relation to privacy in the realm of cloud solutions (Abdullah & Quintero, 2019, p. 602; Ali & Osmanaj, 2020, p. 2).

Indeed, concerns arise about vendors' capability to protect confidential information (Pai & Basu, 2007, p. 41). For instance, data transit throughout the supply chain, the risk of confidentiality breaches increases due to the creation of a data supply chain shared among partner organizations and sub-vendors. Further, metadata that is generated in the data transfer can potentially hold confidential information (Hamlen & Thuraisingham, 2013, p. 3; Almutairi & Riddle, 2018, p. 45; Wulf, et al., 2019, p. 260).

Additionally, striving to balance availability issues by replacing data across multiple data centers might solve the availability problem, but can inadvertently introduce more vulnerabilities to confidentiality due to an increase of people that are handling the data (Wulf, et al., 2019, p. 264).

Confidentiality is put at risk when unauthorized users gain access to cloud solutions, posting one of the primary reasons for confidentiality breaches (Norwegian Ministry of Local Government and Modernization, 2016, p. 15). Furthermore, non-compliance is as well associated with confidentiality breach (Wulf, et al., 2019, p. 260).

An additional area of concern is the legislative part, where governments can access data due to laws, as discussed in the "legal issues" Chapter (KMD, 2015, p. 22; Wulf, et al., 2019, p. 260).

The mitigation for confidentiality issues caused by the supply chain, can be used on security policies and technical measures and control, but this is not sufficient to ensure confidentiality. It is recommended to have comprehensive non-disclosure agreements, SLA, and contract terms (Almutairi & Riddle, 2018, p. 45; Ali & Osmanaj, 2020, p. 10). What can be determined in the SLAs can be authentication and user management, as we will see in the next chapter.

2.1.4.3 Authentication and user management

A critical risk factor that often emerges in cloud solutions is unauthorized access to, alteration of, and disclosure of assets. This often stems from inadequate identity management and lack of password confidentiality (Khidzir, Arshad, and Mohamed, 2010, p. 197; KMD, 2015, p. 15; Pai & Basu, 2007, p. 31). Further, when the system is outsourced, there is a potential risk that untrusted individuals may have access to the solution (Hamlen & Thuraisingham, 2012, p.1).

The process of authenticating users involves more than just external individuals. In fact, internal authorization can also introduce potential vulnerabilities. With the implementation of cloud solutions, the consequences can have more impact due to higher integration of these systems. With high integration opens the opportunity to have a single user management system. If the user management system policies are too strict or not user friendly it can often result from weak authentication practices or non-compliance issues from users, such as misplacing or forgetting passwords (Khidzdir, Mohammed & Arshad, 2010, p. 198; Bachlechner, et al., 2014, p. 56).

The client should assess the balance of access for the outsourcing vendor. It is necessary for the client to offer a suitable amount of access to the vendor, enabling them to fulfill their responsibilities effectively (Dhillon, et al., 2017, p. 457).

To counteract authentication issues, for internal authentication issues it is important that the security measures and policies are not a disturbing factor when enforced (Bachlechner, et al., 2014, p. 56). Externally, the clients should perform due diligence consisting of determining if the service provider provides sufficient customer identity authentication (Pai & Basu, 2007, p. 32).

2.1.4.4 Multi-tenancy security problems

Cloud service providers typically manage an extensive client portfolio, leading to shared infrastructure scenarios. Multi-tenancy is a deployment model where essentially clients are sharing resources collectively from the vendor, and it is a common deployment model in cloud solutions that are classified as private cloud (Ghaffar, 2020,

p. 8; Xiao & Xiao, 2013, p. 844). This setup introduces potential risks to clients' data (Ghaffar, 2020, p. 8; Wulf et al., 2019; Pearson & Benameur, 2010, p. 696; Xiao & Xiao, 2012, p. 845). Specifically, in cloud solutions, it is not unusual for resources to be shared among the clients, resulting in multiple tenants' data being stored and processed on the same physical hardware (Xiao & Xiao, 2012, p. 844).

Without sufficient protective measures, this arrangement could leave data exposed to unauthorized users (Wulf, et al., 2019, p. 260). A typical root cause of this can be the absence of physical boundaries between the data of different tenants, with data segregation taking place virtually. This means that a simple misconfiguration could inadvertently open backdoors or pave the way for privilege escalation, giving adversaries an opportunity to access tenants' data which increases the attack surface (Pearson & Benameur, 2010, p. 696; Wulf, et al., 2019, p. 260; Ghaffar, 2020, p. 8).

Mitigation of multi-tenancy issues are primary getting control over the data lifecycle (Pearson & Benameur, 2010, p. 695). For example, Xiao & Xiao (2012) highlights the necessity of developing new mechanisms to address the security challenges related to multi-tenancy in cloud computing. The proposed solution is to establish clear agreements between the client and the vendor in the SLA regarding the location of endpoints. By explicitly defining the endpoints, the risk of unauthorized access can be minimized, allowing for more effective monitoring. This approach is referred to as collaborative monitoring (Xiao & Xiao, 2012, p. 853).

2.1.4.5 Vendor Lock-in

In the realm of ICT outsourcing, a recurring issue has been vendors crafting their unique standards, such as proprietary data storage practices. This often results in low data portability, making data migration to alternative solutions challenging, if not impossible (Ghaffar, 2020, p. 9; KMD, 2015, p. 18; Dhillon, et al., 2016, p. 456; Seip, 2020, p. 40).

The "lock-in" effect places the client in a weakened position where the cost of exiting the arrangement becomes too big. In worst-case scenarios, organizations may find themselves forced to continue using a vendor’s services, even if there are contract violations or subpar service delivery (Ghaffar, 2020, p. 9).

This vendor lock-in phenomenon presents multiple threats to the organization. For instance, business continuity can be jeopardized if a vendor goes out of business, resulting in a loss of cost control and decreased flexibility in system customization (Kajiyama, et al., 2017, p.651).

To avoid the potential risk of vendor lock-in during outsourcing, it is recommended to establish short-term, annual contracts, providing a chance for renewal. This strategy ensures flexibility and fosters a dynamic relationship between the two parties (Wulf, et al., 2019, p. 262).

2.2 Literature discussion

In conclusion, the adoption of cloud solutions and the outsourcing of ICT systems present several security challenges, including Availability, Confidentiality, Multi-tenancy, Authentication and user management, Loss of control, Due diligence, Legal issues, trust, Lack of user awareness, Constrained market competition, and vendor lock-in. As there are more challenges that appear in the literature, the themes discussed in this chapter are well discussed in the literature. Many of the issues are interconnected and can be root causes for each other. Therefore, mitigation techniques are quite diverse but a common theme that is emergent is that municipalities need to enforce processes that ensure quality for the entire life cycle. The mitigation of these issues is that organizations need to implement measures such as Collaborate and exchange information, push requirements with well-defined Service Level Agreements and contracts, have clear governmental governance with contracts and frameworks, and lastly foster a security-aware culture.

Service Level Agreements as one of the foundations for establishing a legal foundation for defining roles and responsibilities between the client and vendor and that either party meets the necessary security requirements. Others indicate that having clear governmental regulation and strategies, pave the way for organizations to adopt cloud solutions. Lastly, having a security-aware culture ensures that workers process data responsibly and with an awareness that it is in a cloud environment.

Many of the articles go into detail about technical issues and propose a lot of frameworks. I have chosen to generalize the themes or in other words, find common themes, so the literature review addresses the research questions. A lot of the literature addresses the same issues and mitigations, both for outsourcing and cloud sourcing. Organizations that are placing their data outside their organizational boundary can quickly lose control of their data. This lack of control poses a risk to the confidentiality, integrity, and availability of the business continuity. Losing control of the data due to third-party providers (supply chain issue) processing and storing data, or multi-tenancy. Furthermore, the organization lays a great deal of trust in the vendors, and they need to assure that the vendors are enforcing security measures that are sufficient. This can be done with due diligence, but as organizations can have many different contracts, makes it a time-consuming and costly measure. To more external issues such as legal issues, placing data across the border can cause a headache and the further away the more problems arise. Lastly, if there is a power imbalance between the client and vendor, the organization needs to put pressure on the vendor.

Organizations must focus on the importance of having control over their data and systems posed by the challenges of cloud adoption. By addressing these issues or challenges that are proposed by the mitigation techniques, the adoption process can reduce the risk that occurs with cloud adoption. Ultimately, having a proactive approach and focusing on security, privacy and risk assessment can be critical to ensure confidentiality, integrity and availability of the data when adopting cloud solutions.

2.2.1 Research gap

The existing literature in the field of cloud adoption and outsourcing, particularly since its maturation in the late 1980s, offers an array of both conceptual and empirical based models that examine the issue from either technical or managerial perspectives. Despite their depth, a critical gap becomes apparent: many models identify the potential problems in the domain of cloud computing, but few propose robust strategies to forestall these issues, especially when organizations are already entangled in complex situations. The focus of these models remains tilted towards the process of acquisition, and less for the phase of post-acquisition or operational part of the cloud solutions lifecycle.

In the context of my research, the extant empirical studies often single handedly examine individual systems in isolation, thereby missing the complexities of integrated multi-system environments. For instance, in the setting of Norwegian municipalities, the use of diverse systems - potentially up to 200 unique solutions - makes their architecture complex, compared to a business organization that buys for example an ERP-system. The diversity of these systems, combined with the variability of available resources and the size of municipalities, creates a unique niche that is currently under-explored.

Addressing all these parameters or factors could contribute to bridging the current research gap between typical security issues in cloud adoption and the diversity of cloud system usage. The goal is to develop an abstract, generalizable model that caters to the diverse and complex realities of modern cloud computing environments. This model could serve as a reliable guide for understanding and mitigating security issues inherent in cloud computing adoption.

3 RESEARCH METHODS

In this chapter will delve into the different methodological approaches that are used to retrieve and analyze the data to perform empirical investigation. Firstly, it commences an implementation for the systematic literature review process, highlighting the process that is used to select and synthesize relevant research that exists in the current field that will be explored. The next part will consist of a rationale for adopting a qualitative research methodology, which will emphasize the value of using such an approach. The chapter elaborates on the data collection process, specifically detailing the use of semi-structured interviews as a means of gaining in-depth information from the interviewees. Finally, the data analysis techniques employed to interpret and draw meaningful conclusions from the gathered information are explained.

3.1 Literature review

Conducting a Literature review is essential to academic research (Xiao & Watson, 2019, p. 93). This process involves of looking back on what has previously been done on a topic where it demonstrates knowledge and understanding of the existing literature on the given topic. It is through this analysis that new knowledge is built up on the foundations of previous literature. When applied it will provide insight into an in-depth understanding of the current landscape of cloud adaptation in municipalities and the problems that come along with it (Paré, Trudel, Jaana & Kitsiou, 2015). Beyond just an accumulation of information, a literature review is also about critical evaluation, for example, seeking gaps and weaknesses in the literature. This is what differentiates a literature review from a report. The aim of the literature review is to cover the objectives of existing research, theories, and evidence, as well as evaluate and discuss the content of the literature (The University of Edinburgh, 2022).

3.1.1 Research strategy

For this thesis a methodological literature review will be conducted. The methodological literature review aims to outline the strengths and weaknesses in the existing literature. The methodological approach chosen in this thesis will be based on Xiao & Watson's proposal of a systematic literature review (SLR). They propose a comprehensive approach to conducting a literature review based on Okoli & Schabram. The method's purpose is a methodology that covers many of the disciplines of the complex field of information system research (Okoli & Schabram, 2012).

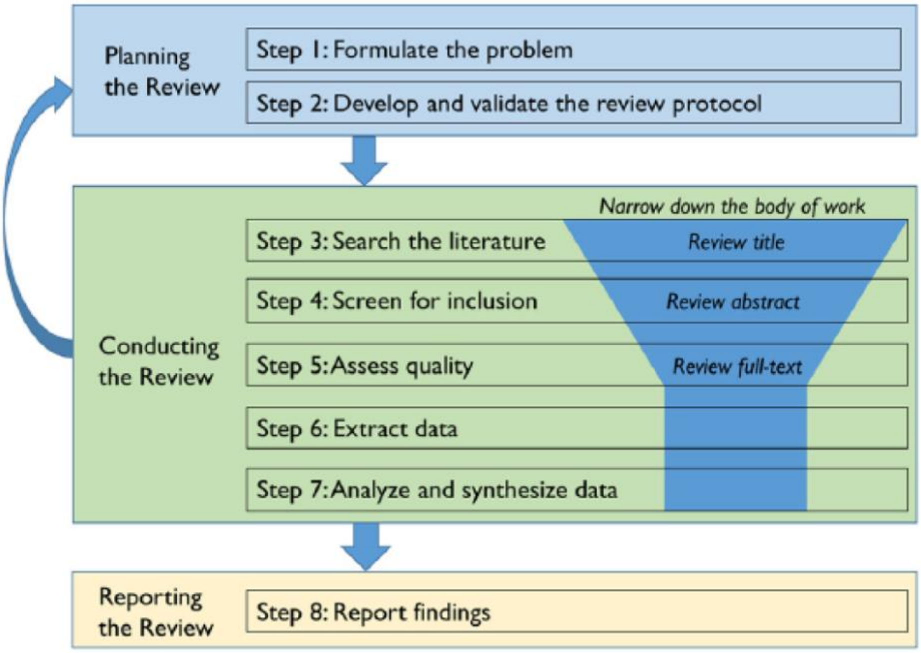
Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Conducting the Review
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 1 Process of systematic literature review (Xiao & Watson, 2019, p. 103)

A literature review consists of three stages, according to Kitchenham & Charters (2007). The first part is Planning which consists of; Planning the review, conducting the review, and reporting the review (Kitchenham & Charters, 2007). Furthermore, these can be broken into eight different phases (see *Figure 1*).

3.1.1.1 Planning the review

The first part of the process is to **Formulate the problem**. To conduct a literature review, you seek to get an answer to a problem. The research question for this thesis is the problem seek to get an answer to. When you formulate the problem, it defines the scope of the project, reducing the risk of getting irrelevant information during the literature review. It is an iterative process where most of the steps are about exploring the topic. As I continue my approach, the research question will change according to my exploration of the literature. At the start, the research question tends to be rather broad. During the process, the research question will become more specific and refined. In the end, my goal is to be able to have an answer to my research question (Xiao & Watson, 2019).

The scope of the literature review, which are deemed as suitable for the research question, is research papers that focuses on ICT-Outsourcing. The literature review will first explore this domain, and further delve deeper into the field of cloud computing. The reasoning for this approach stems from the fact that outsourcing is a well-established field. It has been extensively researched since the late 1980s. On the other hand, cloud computing, which is a form of outsourcing, is a relatively new area. Therefore, in conducting the literature review, I first tackle the secondary field of ICT-outsourcing, following transitioning to the primary topic of interest: cloud solutions.

The second step is to **Develop and Validate the Review Protocol**. This is where you set a plan to specify the methods used during the literature review. It ensures that there is quality to the review. This is because it minimizes the risk of having a bias in the data selection and analysis. The review protocol should explain the search strategies, quality assessment, synopsis, reporting, and criteria for inclusion (Gates, 2002). This has made the process has intentionally improved my efficiency tasks minimized redundant work. The implementation of the protocol has assured a sustained focus on the topic. It has facilitated a systematic approach in identifying literature that are relevant to the field that I am exploring. The review protocol can be seen in Appendix C: **Error! Reference source not found.**.

3.1.1.2 Conducting the review

When conducting the review, the first step is to **search the literature**. This is where the literature search will provide material for the review. There are three ways one could go forward. The methods are database search, backward search, and forward search. It is natural in our context to perform database searches in electronic databases. Then you can supply by performing backward searching. This is by looking at references used in a research article. The last method is to perform forward searching. Forward searching is by looking at cited articles in each journal. Most of my literature search has been done by searching electronic databases. I ended up using several electronic databases. This is because no database yields enough relevant results. In section **Error! Reference source not found. Error! Reference source not found.** describes the criteria, electronic databases, and the keywords that were used. I screened the title to filter out irrelevant articles in this step (Xiao & Watson, 2019).

After performing the literature search, the next step is to **Screen for Inclusion**. When all the references were compiled, the articles were screened. This process helps me decide what articles should be included. The review protocol, which can be seen in section **Error! Reference source not found. Error! Reference source not found.**, lists specific criteria that determine whether it is relevant. In this part, the literature is screened by reading the abstract of the article. This makes it easier to rule out irrelevant articles, without spending too much time on it later in the process (Xiao & Watson, 2019).

The fifth step is **Assessing quality**, which involves obtaining the full text of the articles. Screening the full text enabled me to refine the selection of articles. This step is the final stage before preparing the data extraction and synthesis of the data. It is the last stage to rule out any articles that are irrelevant to the research question, which are based on my inclusion criteria which can be seen in **Error! Reference source not found. Error! Reference source not found.** (Xiao and Watson, 2019).

The sixth step is **Extracting Data**. This is where all selected articles are structured and organized into a table. This information can be seen in *Table 7 Literature List*.

Once the data extraction is finalized, the next step is **Analyzing and Synthesizing Data**. This step entails combining the data from the research using the proper quantitative, qualitative, or both methodologies. This is the part where I read all the relevant articles and highlight significant findings of the reports, a process called "coding". For this process NVivo will be used to analyze the articles in a structured way.

3.1.1.3 Report the review

The last step is to **Report findings**. When the systematic literature review process is done, it should be reported in a detailed way so that it is possible to reproduce the result. The most important thing to include is the criteria and the rationale behind it. I have created a flowchart as seen bellow in *Figure 2* according to Xiao and Watson that illustrate the process of my literature review (Xiao and Watson, 2019).

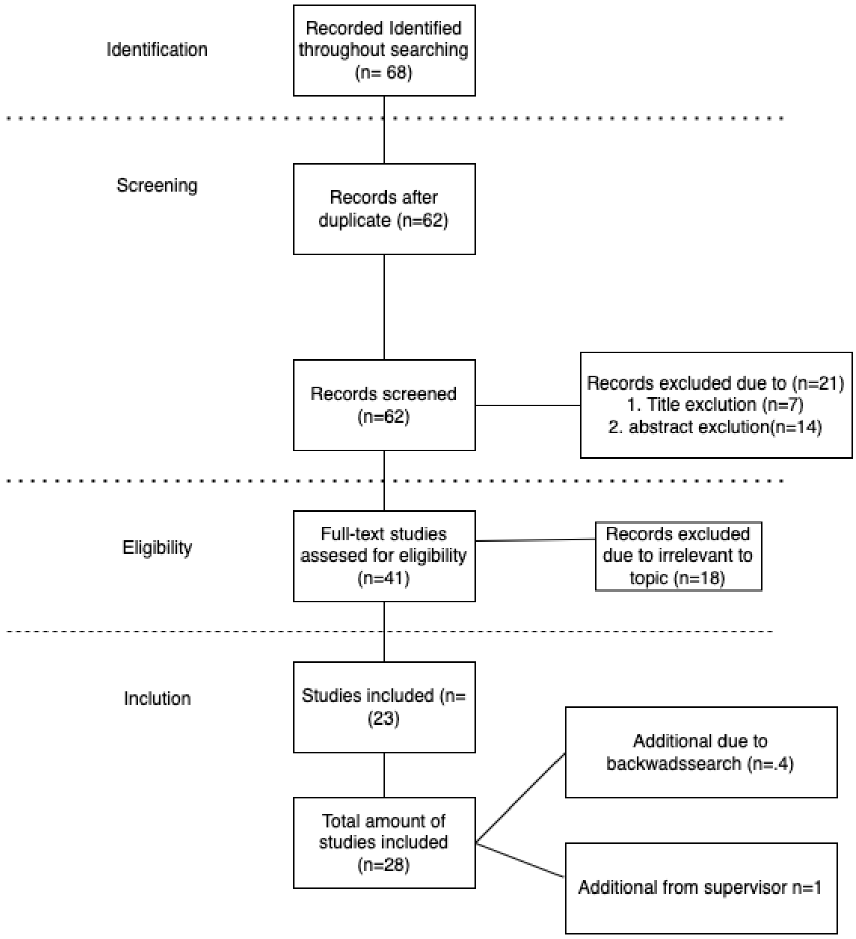
Identification
Recorded Identified throughout searching (n= 68)
Screening
Records after duplicate (n=62)
Records screened (n=62)
Records excluded due to (n=21) 1. Title exclution (n=7) 2. abstract exclution(n=14)
Eligibility
Full-text studies assesed for eligibility (n=41)
Records excluded due to irrelevant to topic (n=18)
Inclution
Studies included (n= (23)
Additional due to backwadssearch (n=.4)
Total amount of studies included (n=28)
Additional from supervisor n=1

Figure 2 Literature search and evaluation for inclusion (Xiao & Watson, 2019, p. 108).

3.2 Qualitative research approach

Qualitative strategies are procedures that often include research methods such as case studies, ethnography, and phenomenology, which often emphasize the focus on qualitative data. The most used qualitative research method that is used in IS research is a case study (Recker, 2021, p. 123).

A case study focuses on an instance of a phenomenon that will be investigated. Especially when the boundaries between the phenomenon and the context are not clear. It is designed for instances where variables are more of interest than data points (Recker, 2021, p.123). The case study gives an in-depth description of an instance compared to other strategies, such as surveys that tend to have a much broader, but more shallow exploration area. The case study has its advantages such as the setting being natural, and the processes and relationships of the whole environment. There are both exploratory and descriptive approaches to case studies (Johannesson & Perjons, 2014, p. 144).

A case study does not necessarily need to be bound to one single instance but look at several instances (Johannesson & Perjons, 2014, p.144). This is called a multiple case study, enabling you to look at several cases to investigate the same phenomenon (Yin, 2017). The multiple case studies' purpose is to replicate the phenomenon and compare the findings. This approach makes it more compelling because its findings are considered more robust compared to a single case study (Yin, 2017, p. 55).

The research questions are looking at the security/privacy barriers to adopting cloud solutions. The context will be the Norwegian municipalities, and the phenomenon will be the barriers. I have therefore concluded that the suitable research method in the qualitative approach will be a multiple case study.

3.2.1 Research design

The desired outcome of this article is to identify the obstacles that Norwegian municipalities encounter during the adaptation of cloud solutions. This will be useful for workers who are making these decisions in different municipalities. This emphasizes the targeted audience, managers who make decisions and are responsible for adapting new technology in Norwegian municipalities. This exploratory research applies qualitative research methods. The targeted audience is quite focused, and the selection between quantitative and qualitative research approaches makes the quantitative approach problematic in terms of the limitation of the sample size of the responders.

The initial aim is to get an in-depth mapping to identify the obstacles which a qualitative research approach enables me to achieve. The research approach is going to use inductive reasoning throughout this article. Inductive reasoning has been used to strengthen my collected textual data into a more unified summary that can result in reliable data. The primary purpose of using inductive reasoning in our approach is to allow frequent or significant themes from the interviews without the restraints that typically come with structured methodologies (Thomas, 2006). In my case, there are three main purposes of the appliance of inductive analysis approach:

1. To condense the transcripts into a summary format.
2. To establish links between the research question and the findings from the transcripts and ensure that the links are transparent and defensible.
3. Be able to explain the underlying experiences and processes from the transcriptions.

(Thomas, 2006, p. 238).

3.2.1.1 Case design

As previously indicated, the case study design will be employed to conduct the research for this project. I have used Robert Yin's thorough manual, "Case Study Research Design and Methods" (Yin, 2003). An embedded multiple case study is the approach case study design that was chosen for this project. The justification for this is that looking into many facets of each case allows for the collection of richer and more nuanced data, which leads to a deeper knowledge of the complexities involved in cloud adoption and the resulting security issues and how to deal with them. By considering many components of the subject, this design also offers a holistic view of the study challenge by highlighting patterns, correlations, or interactions between distinct elements. It also improves the transferability of findings, allowing for insights that may be applied to a wider range of contexts, by looking at multiple aspects within each instance (Yin, 2003, p. 49).

The replication strategy I will use for this thesis is the theoretical replication logic proposed by Yin (Yin, 2003, p. 49). What this means in practice is that the selection of suitable candidates is based on parameters and factors on how they experience security issues in cloud adoption. The factors or parameters that are used are Organizational resources, size, structure, and cloud adoption stage.

3.2.1.2 Data collection

The empirical data collection technique to be used in this project will involve conducting qualitative interviews. As a well-known qualitative data collection technique, interviews serve as "conversations with a purpose." The targeted organizations will be municipalities and inter-municipal ICT collaboration organizations. Interviewees will be required to have experience with ICT-system acquisitions and ideally be responsible for the organization's cybersecurity. Data collection is planned to span one month or until data saturation is achieved. To find suitable subjects, the top IT manager in each municipality will be contacted.

The semi-structured interview method will be employed, as it allows for gathering detailed information about municipalities' obstacles when adapting to cloud solutions. The unstructured nature of these interviews enables further exploration of topics relevant to the problem statement. An interview guide, consisting of questions based on research questions and literature review findings, will be created, and can be found in Appendix B.

The interviews will be conducted digitally via Microsoft Teams. With consent from the subjects, interviews will be recorded to facilitate transcription. The project is approved by the Norwegian Centre for Research Data (NSD), where it has been assessed for processing of personal data. The expected duration for each interview is approximately 45 minutes, which aligns with the typical timeframe for a semi-structured interview (Jamshed, 2014). The Consent form are accessible in Appendix A.

The plan is to have around 8-10 interviews as that is estimated because of the case design mentioned earlier as well as to reach saturation in the data collection. Data saturation refers to the point at which new information from additional informants becomes redundant, as similar findings have already been gathered from previous informants. At this stage, the collected data is deemed empirically sufficient to draw conclusions (Grady, 1998, p. 26).

3.2.1.2.1 Semi-structured interview

During the interviews I will utilize a semi-structured interview method. This is because as mentioned in the case design it is suitable to have a rather exploratory interview so I can dwell into topics that are interesting to the research question. One attribute that I will focus on is ensuring trustworthiness and reliability in the data that I collect during the interviews. I have chosen to use a framework that is proposed by Kallio et al. (Kallio, Pietilä, Johnson & Kangasniemi, 2016, p. 2954). This framework or guide introduces fine steps for creating a semi-structured interview guide, on which I base my interview guide on (See Figure 3).

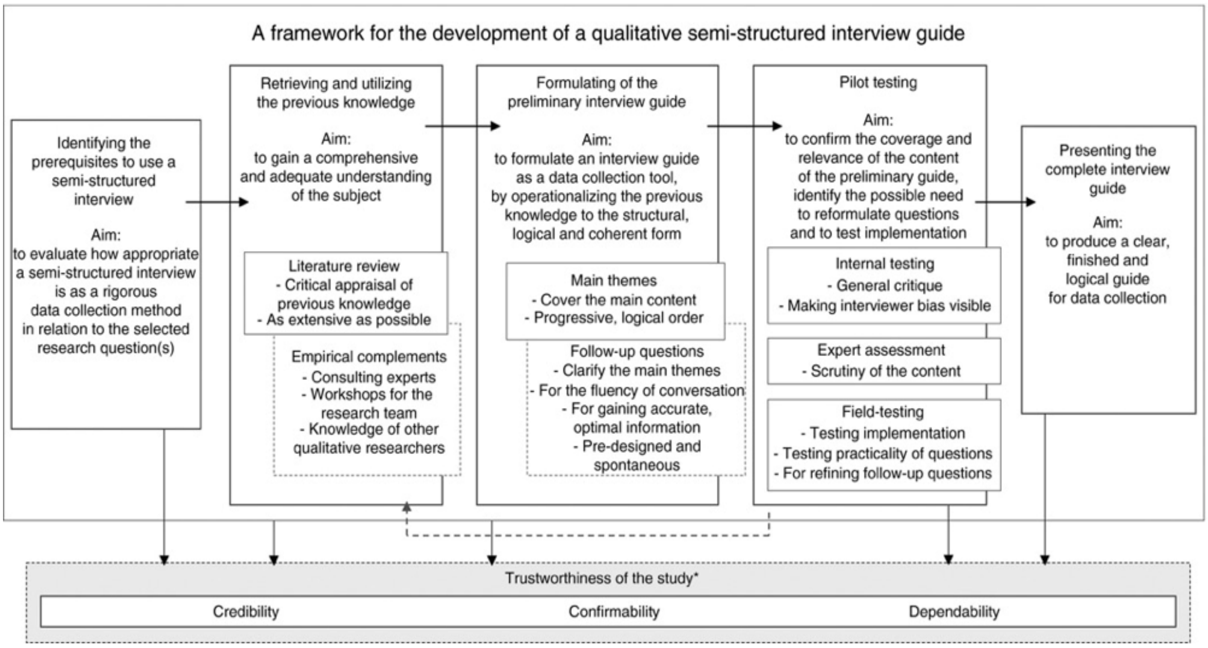
A framework for the development of a qualitative semi-structured interview guide
Identifying the prerequisites to use a semi-structured interview
Aim: to evaluate how appropriate a semi-structured interview is as a rigorous data collection method in relation to the selected research question(s)
Retrieving and utilizing the previous knowledge
Aim: to gain a comprehensive and adequate understanding of the subject
Literature review - Critical appraisal of previous knowledge - As extensive as possible
Empirical complements - Consulting experts - Workshops for the research team - Knowledge of other qualitative researchers
Formulating of the preliminary interview guide
Aim: to formulate an interview guide as a data collection tool, by operationalizing the previous knowledge to the structural, logical and coherent form
Main themes - Cover the main content - Progressive, logical order
Follow-up questions - Clarify the main themes - For the fluency of conversation - For gaining accurate, optimal information - Pre-designed and spontaneous
Pilot testing
Aim: to confirm the coverage and relevance of the content of the preliminary guide, identify the possible need to reformulate questions and to test implementation
Internal testing - General critique - Making interviewer bias visible
Expert assessment - Scrutiny of the content
Field-testing - Testing implementation - Testing practicality of questions - For refining follow-up questions
Presenting the complete interview guide
Aim: to produce a clear, finished and logical guide for data collection
Trustworthiness of the study*
Credibility
Confirmability
Dependability

Figure 3 The phases of a semi-structured interview guide development based[2]

The first phase is about evaluating if a semi-structured interview method is suitable for data collection in this project, this is already argued previously. The second phase is

[2] "The phases of a semi-structured interview guide development based" [Figure]. 2016. By Kallio, Pietilä, Johnson & Kangasniemi. Retrieved from: https://onlinelibrary.wiley.com/doi/10.1111/jan.13031

about formulating a preliminary interview guide based on previous knowledge and literature. By this time, I already have performed two structured literature reviews that I could base the information on and make preliminary interview guide questions based on that. The third phase is about refining the guide to ensure the balance between main themes and follow-up questions. In this phase, I had created roughly 19 preliminary questions that were used as a guide to the dialogue during the interview towards my research question. (See appendix B). After the creation of the interview questions, I proceeded to perform pilot testing, which is in phase 4. The initial aim of conducting a pilot interview is to see if the questions cover and have relevance. Reflection and feedback from peers enabled me to improve the interviews. After I completed the review, I made informed changes and adjustments to the interview questions, directly improving the quality of the interview guide (Kallio et al., 2016, p. 2960).

3.2.1.3 Ethical considerations

When planning the interviews, it was necessary to send an application to NSD. NSD is responsible for managing research projects and providing archival services for research data. For a research project conducted in Norway, researchers need to obtain NSD approval, before collecting and processing potentially private sensitive information. For my project, I ensured that my thesis received approval from NSD (reference number 896318), before collecting any data. Approval from NSD ensures that the data-gathering procedures are acceptable.

The informants are informed of the procedures, and each participant signed a consent form (see Appendix A). The form emphasizes that it is voluntary to participate, allowing participants to opt-in or out of the project at any time. It also consists of the details of the anonymization of the data and the deletion of the voice recording from the interviews. I retain only the responses and a description of the type of municipality the informant worked for. The research remained unbiased, with the findings accurately representing the answers provided by participants.

3.2.1.3.1 Quality assurance

To make sure that the data collected retains the quality, as mentioned I will use the framework proposed by Kallio et al. One of the benefits of that framework is that it ensures the objectivity of the trustworthiness of the data collection process. Lincoln & Guba proposed that the factors that contribute to trustworthiness are credibility, transferability, dependability, and confirmability (Lincoln & Gauba, 1985, p. 219). To ensure credibility I spent this whole year discussing with peers (students, supervisors, and colleagues) discussing the domain I am studying. Prolonged Engagement and Peer debriefing aid me to achieve credibility (Lincoln & Gauba, 1985, p. 304). Transferability was achieved by something called Guba's “Thick Description” which explains the phenomenon in detail, which the literature review was for me (Lincoln & Gauba, 1985, p. 359). To achieve transferability, I had my supervisor as well as two fellow students evaluate my collection or perform external audits. Lastly, the confirmability was achieved by external audits and has a sufficient audit trail (Lincoln & Gauba, 1985, p. 319).

3.2.1.4 Data analysis

The data analysis of the data that is collected from the interviews will be done in a structured manner to ensure that all the themes that are relevant to answer the research question are covered from the interviews. It is important to do it in a structured manner since there is a lot of textual data that is to be covered. Specifically, I choose to follow the process described by Braun & Clarke. The process I will follow is a thematic data analysis (Braun & Clarke, 2006). The process consists of the following processes:

- Step 1: Become familiar with the data: Immersing yourself in the data by reading the data repeatedly and actively searching for patterns is crucial for qualitative research analysis, as it forms the foundation for subsequent coding and identification of themes, regardless of the specific analytic approach. In this stage, interviews are transformed into written form.
- Step 2: Generate initial codes: To generate initial codes from the data after familiarization, organize data into meaningful categories, and identify interesting aspects that could form repeated patterns or themes across the dataset.

- Step 3: Search for themes: in this phase, the focus shifts to organizing codes into potential themes, examining their connections, and using a thematic map to explore the main themes, sub-themes, and their relationships with one another.
- Step 4: Review themes: is to define themes by reviewing coded data extracts, ensuring internal coherence and the external distinction between themes. Here I can rework the themes as needed to create an accurate thematic map that reflects the data set's meanings.
- Step 5: Define themes: Involves defining and refining the themes from the previous steps. The goal is to have themes that capture their essence, conduct detailed analysis, and identify sub-themes.
- Step 6: Write-up: to report the findings. It is important to write a concise, coherent, logical, non-repetitive, and interesting report that effectively tells the story of the data and demonstrates the merit and validity of the analysis. (Braun & Clarke, 2006, p. 16-23)

In more practical terms I will first need to transcribe the raw data from an audio file. It is time-consuming to transcribe the raw data into raw textual data. I will use Microsoft Word Online, which has an automatic transcription tool that can automate much of this process, but it still needs manual assessment to transcribe accurately. When the data was transformed from audio format to textual data, the way I will work with the textual data to find themes is to perform the coding. Coding involves assigning labels to chunks of raw text (Recker, 2021). The coding highlights the important points that I can put into unified themes as described in the thematic analysis process. It will aid me to break down the textual data into meaningful information. There are three parts to analyzing qualitative data. The first one is data reduction which is about reducing the data to make it manageable (Miles & Huberman, 1994). I use a tool called NVivo 2020 that enables me to transform the data into meaningful data. I disregarded irrelevant data by assisting its relevance to the research question. The second part of analyzing the data is data display which refers to reducing the data. This can typically be done by coding the data. I could categorize the transcribed data by simply placing them into “bins” or tagging them into suitable categories. The last part of analyzing the qualitative data is conclusion drawing and verification, which is about developing conclusions and verifying them from the data that has been analyzed. This is done by iteratively looking at the raw textual data and comparing it to the findings in the literature review (Miles & Huberman, 1994).

3.2.1.5 Sampling

To ensure the collection of high-quality and meaningful information from the interviewees, it is essential to define relevant interview subjects to my empirical data collection. The subjects need to take actively part in decision-making regarding cloud computing adoption within their respective municipalities, is what I have identified as most relevant. This includes individuals responsible for the security of systems that are utilizing cloud computing.

To maintain the validity of my research, I will conduct six interviews, which seems to be adequate given that each interview lasts approximately 45 minutes. The aim of the interviews is to provide me with in-depth insights and unique experiences, ultimately helping me to address the research question effectively.

The Job title and role in the organizations of interviewees varies from one municipality to another, but they typically hold responsibilities over the organization, operations, acquisitions, or IT-security within the municipality. Moreover, the observed differences among the municipalities, demonstrating the nuances of their individual characteristics, allow for a more robust generalization, thereby enhancing the credibility and applicability of my findings. In the following Table *2* you will find the roles within their respective organizations for each informant. For the sake of anonymity, every informant has been assigned a unique number, from one to six, each signifying a distinct municipality or inter-municipal organization.

Table 2 Informants role

Informant number	Organizational function	Size organization
I1	Responsible for the security	Small municipality
I2	Head of IT-department	Medium-sized municipality
I3	Responsible for the security	Medium-sized municipality
I4	Head of operation	Intermunicipal collaboration organization (large)
I5	Responsible for the security	Intermunicipal collaboration

		organization (large)
I6	Responsible for the security	Medium-sized municipality

4 EMPIRICAL FINDINGS

Upon examining and analyzing the data, I have reached some findings related to the research question. This will be discussed in this section. As the interviews are quite broad, there have been several themes that are not mentioned in this chapter. This is because they were not discussed sufficiently to be deemed a significant finding. The findings will include quotes that use the numeration from I1-6 as according to the informants in Table *2*. The quotes are highlighted in *italics* to emphasize and make them more readable. The quotes are translated into English because all the interviews were conducted in Norwegian. Therefore, there is some room for interpretation. Lastly, at the end of this chapter the findings are summarized in Table 3.

4.1 Organizational challenges

4.1.1 User compliance

One challenge that was apparent in the adaptation of cloud solutions was how the employees behaved toward the cloud solution. As the system grew more integrated and larger the consequences are increasing. I5 mentioned that having an increase in integrated systems makes it hard for user management. Where a common issue was:

"Accounts with re-used passwords that have caused people to breach a couple of municipalities."

The users of the municipalities are so diverse ranging from elementary school children to elderly people, it makes it hard for municipalities to manage the users of these systems. Another issue about user compliance is the employee's attitude towards data. I2 illustrated a scenario where a department used Microsoft Teams which stored and processed data outside of Norway. If employees sent sensitive information, it could breach the Norwegian archival act so they had made a rule that no sensitive information should be stored or processed in Microsoft Teams. As I2 argued that:

"In practice, it is possible to enter sensitive information in Teams. But it is in our procedure that employees should not use Teams for sensitive information."

So, the issue remains you cannot completely protect yourselves from employees that either choose to disregard or are knowingly breaching the policy which poses a risk of leaking confidential data. This highlights the importance of informing the employees, in other words performing security awareness training on the employees, as several informants said they continuously performed.

4.1.2 Collaboration

Due to the nature of how municipalities are organized, each of them is responsible for acquiring and operating IT systems. Some of the largest municipalities collaborated with smaller municipalities as I2 said:

"In small municipalities, it is often the case that people have so much responsibility that they never become good at anything. Buying cloud services is a separate competence. We have spent time building that expertise."

Small municipalities typically have limited resources, sometimes only one or two responsible. These municipalities may have issues developing expertise to acquire cloud solutions in a secure manner. Therefore, these municipalities are reliant on collaboration from other instances. On the other hand, one municipality (I3) was a former part of an inter-municipal ICT-collaboration and the reasoning for them exiting that collaboration was that:

"Exiting the inter-municipal cooperation was also the opportunity to decide for yourself and get a little faster innovation. That you can come up with new solutions more quickly and operate innovatively."

It is apparent from several of the interviews that the cooperation could be bureaucratic and slow, which affected the process of innovation. Even though collaboration could improve the acquisition process, thus improving the security of the cloud solution, it could slow down the cloud adoption process in general. This, in turn, significantly impacts the overall security of the system, as the absence of adopting new solutions becomes a critical factor. This is particularly important considering that the legacy system may not offer the same level of security. There have been collaboration projects from higher instances such as counties or departments on solutions (that run on the cloud) for many municipalities. All the informants expressed that they were positive about such projects. For example, I4 expressed:

"I have great faith in it when it comes to ensuring the smooth functioning of data flows and establishing a centralized location for managing IT and professional security within the healthcare sector, rather than each individual municipality having to tackle these issues independently."

Health data has proven to be difficult to move to the cloud due to the nature of the cloud solutions, and maybe this is the effective way to get such systems up to the cloud due to the nature of the resources that it requires. It is worth mentioning that many of the projects that were mentioned are highly profiled media cases such as "Nordkart" which was subject to data leakage or "Helseplattformen" which has been a disaster in terms of cost and functionality. The impact of collaboration efforts on security improvement can be a subject of debate. One aspect to consider is the potential for complex bureaucracy due to the involvement of numerous people in the project.

4.1.3 Conflict of interest

Although municipalities are organized quite differently, every organization has essentially a project owner, purchasing manager, IT department, and a Councilor (which is the main responsible person for the cyber security of the municipalities system). From many of the interviews, the project owner could potentially be a person who has little competence in security or IT. As I5 expressed:

"After all, the project owners prioritize functionality, which leads to a different perspective. This raises the question of whether functionality should outweigh security. Those of us working in security are opposed to such prioritization."

Such internal conflict of interest can become a tug of war between the project owner and the IT department. As some project owners disregard the cloud solutions or can act opportunistic. Two of the informants said that they either are initiated too late in the process or are neglected or down prioritized. As expressed by I4:

"It is unnecessary for the IT department to assess this solution. Since it is a cloud-based solution, all that is required is to get the user credentials, and then you are ready to use the system."

This ends up with a project owner acquiring a cloud solution without assessing any parts of the security- or technical aspects of the system, which can possibly be a large security risk. Systems with poor security, or violation of data privacy can be implemented and integrated into the existing environment of the municipality. As one stated, when the IT-department is not included the critical or important questions to the vendor are not asked. Indicated by I5:

"Are identity controls implemented to manage authentication and access? Are regular backup routines established? What security processes are in place? How is the system monitored? What is the system's uptime?"

What causes owners not to involve the IT-department is hard to say, but as I3 indicated that:

"The project owner involves us only when there are large projects, or it requires technical skills."

Implying that departments may feel neglected. This could be attributed to the perception that involving the IT department may introduce complexity and be seen as a barrier to innovation.

Lastly, it can be how the organization is organized, where the IT department is separated, especially for inter-municipal collaboration creating a physical and mental barrier for the project owner to involve the IT-department. As I5 expressed:

“We often feel that X organization as a municipality's IT department, but it is a separate organization, we come to be seen not as internally as if we had support in the municipality in a way. Therefore, we often enter the process a little late, and that is a challenge.”

Another aspect that the IT-department experienced is that the communication between the IT-department and the Privacy Commissioner was not proactive. I2 expressed:

“The data protection officer says: "no, that doesn't work". Well, what can I do then?”

This forces the IT-department to find solutions and use a lot of resources on that. The IT-department must assess and outweigh the risk on their own, while constantly being set constraints when acquiring the system.

4.1.4 Executive Involvement in Cloud Security Adoption

One of the most cloud-mature municipalities in Norway experienced that how well they adopted the systems in a secure manner was heavily reliant on how seriously the Chief Municipal Executive took cyber security. As I2 expressed:

“I feel that we have a municipal management and a municipal executive director who are very good. (....) After our old one retired, there has been a big change because he addresses information security, and is concerned with it, and then it (security) also spreads a little across the whole organization. (...). The previous municipal executive director never cared. He had only said “yes” if we proposed the safety regulations without discussing it with us.”

Management's involvement in security and in digitalization is almost a no-brainer for successful digitalization, but it is essential to get involved in security as there are countless issues that arise when adopting cloud solutions. On the other hand, all municipalities have a cloud-first strategy, what does that mean? As I5 stated:

"There are a lot of things a little higher up in the system and municipal management that do not know about IT. Then it was said that our strategy is "cloud first". My question is on what terms?"

It appears that the management creates abstract strategies and guidelines that do not resonate down the organization. If management does not understand how costly, or how big risks it takes to take certain systems it can quickly become an issue.

4.1.5 Resources

One of the root causes for barriers to adopting cloud solutions for municipalities is the resources it takes to adopt it. Municipalities can often have 100-300 different systems that they maintain. If all these systems need to be assessed whether they should be migrated to cloud solutions. As I6 mentioned:

"And when the systems are migrated to the cloud, it can become quite chaotic. Employees may find themselves having to adapt to a new platform and undergo training. This poses a challenge when municipalities transition to the cloud, as unexpected situations may arise that require the use of alternative professional systems. In such cases, there is often a lack of sufficient time for proper training, particularly when it comes to cloud solutions."

This illustrates how resources it requires to migrate to cloud solutions, and it can quickly go over budget if, for example, someone explores that the data cannot be processed by the system. As well the amount of proper training can be comprehensive considering some of them might have little motivation to learn the new system. This financial aspect is closely tied to the political landscape of municipalities. As I1 expressed:

"A lot of budget and money is dependent on politics in municipalities."

Meaning that there needs to be a political will to adopt cloud solutions, and most importantly the political board is willing to prioritize security. These people are "lay people" who are ordinary people who potentially do not have any experience in technology or security and might see the functionality and cost as a more important part rather than the security. It is important to note the diverse range of services that municipalities are responsible for providing. For example, I2 illustrated:

"In the municipal sector, we have an extremely large number of services to be delivered. There is a large requirement for documentation, in addition, there is also many applications, which are based on the type of services they are to be used for."

It describes how much is in motion to acquire cloud solutions. This number of resources it takes may contribute to difficulties in adopting cloud solutions and prioritizing security, particularly when decision-makers can have limited experience in technology or security. How do municipalities have the resources available to do this? One from a small municipality that had little collaboration with other municipalities, which was I1 stated that:

"It may be that we take consultant help if there are things, we are unsure about that you have not come across before."

As well as other municipalities stated when they did not have the resources available, they sourced people to do for example IT-architectural analysis or legal consultants to know if they were in the clear to use the cloud solution. The downside to this is that consultants are much more expensive compared to in-house. On the other hand, cloud solutions are a form of outsourcing the system and its operation which potentially be a resource reliever as expressed by I2:

"At the same time as more and more goes into the cloud. It relieves us from the burden of operating the system. So, we can use more time on consulting part of the organization."

Migrating to the cloud can potentially lead to a more efficient use of IT-resources and enable the IT-department to have a more strategic and proactive role in the organization. Simply by freeing their resources from in-house operation, they can use their time on for example securing their systems.

4.2 Strategic and Operational Planning

4.2.1 Guidelines, strategies, and Frameworks

All the informants mentioned that there were too many guidelines to relate to. As I2 pointed out that:

"It is challenging to have a cohesive strategy since we are using several strategies. It ends up that we are dealing with multiple fragmented pieces of different strategies. I think. Instead of more strategies, we need fewer. Sometimes it feels like the people in the ministries are paid based on the number of words they write."

Almost all of them had a joke on this topic when asked about what they thought about guidelines, illustrating that there is a bureaucratic issue when creating those guidelines. Not having one guideline can lead to holes in the implementation and ultimately the security of the systems as there is no assurance that they satisfy all the requirements of the guideline. It is not only an issue that there are many guidelines but several expressed that their guidelines were not concrete enough and only at a managerial level. As I6 mentioned:

"There are an incredible number of guidelines which have big words at a strategic level, but very little about implementation."

This poses a significant problem in the context of system security, and how to implement the cloud solutions properly. As the level of technicality required to implement solutions increases, vague guidelines become less valuable and inadequate in providing effective direction. This becomes an even bigger issue when there are fewer resources available, for instance in small municipalities without any collaboration efforts. Another issue expressed is that the guidelines were difficult to find. As expressed by I6:

"KS (Municipal organization) managed to finally come with a supplier class list within the school which is practically almost impossible to find."

Then you have the combination with too many guidelines, too vague and they are difficult to get a hold of to implement cloud solutions successfully and securely. This increases the likelihood that the systems are not implemented properly.

When it comes to guidelines there is a known dispute between the Norwegian Digitalization Agency and the Norwegian Data Protection Authority which have two different opinions on how to guide municipalities on the Cloud Act issue. As I4 mentioned:

"Digdir believed that it was not considered as a data transfer until the USA extracted information, while the Norwegian Data Protection Authority said that as long as there is an opportunity it is considered as a data transfer."

Different authorities contradicting each other makes it not easy for municipalities to know whether they are in the clear or not. It can lead to inconsistency in the security of the systems and at a managerial level led to key security measures being overlooked. Further expressed by I2:

"When it comes to national strategies and national appeals. Which is written a bit like a ministry here and a ministry there, so it seems like they did not talk to each other when they wrote it."

When different governmental instances are not unified and are not collaborating with each other it comes to lack of clear guidance. With a lack of unified guidelines from the agencies, municipalities could find themselves to be non-compliant, leading to potential legal risks.

The need for clear guidance is expressed by the informants. As expressed by I2:

"I think it would have been easier for us then, if there had been such central guidance, because now we have to sort of sit and assess ourselves."

To have uniform guidance, relieve the resources that it takes to make decisions and assess for the municipalities. For example, having one person in a municipality of four

IT-employees to sit and assess whether they should use Microsoft services, because of fear of the Cloud Act can quickly become a pothole for resources, and you could argue that those resources could be spent better than that.

A voluntary organization called KiNS[3] has recently gained traction and has shown good results, where they have gotten somewhat a uniform guideline and framework for adaptation of cloud solutions. As mentioned by I6:

"The framework I mention from KiNS is one of the few that actually asks some specific questions about, for example, whether you have a geo-redundant backup so that if the data center burns down."

Maybe this removes the bureaucracy and speeds up the process when it becomes a "private" initiative rather than governmental initiative. There is a need for proper guideline and framework for municipalities to become effective and have a successful implementation and ensure that they comply with the security requirements. However, sadly it seems that there is a long way to go to have a uniform guideline or framework to adapt to cloud solutions.

4.2.2 Contract follow-up

Post implementation or migration to cloud solutions needs to have a contract follow-up to see how the vendors perform according to the contract. Performing contract follow-up requires competence. However, due to the nature of how municipalities work, the responsibility to perform contracting follow-up usually falls on the system owner. As mentioned by I2:

"After all, it is the system owner who must first and foremost follow up on the agreement of the vendors. Then they must set aside time to do it. It must come instead of and not in addition to already existing tasks. And then it's easy to point out. So, we can say to the system owner "do a vendor follow-up. So, they don't really have the

[3] KiNS is an *association for municipalities that function as a forum for infosec*

knowledge to perform the follow-up. So, the system owners are not prepared for the role."

The issue is that the system owner is not suited for the job to perform contract follow-up. It requires competence to be able to follow-up on the contract. The contract follow-up is a key challenge, as it is critical to have contract management to ensure data is managed according to the agreement, including those related to data protection, are adhered to. I2 argued that:

"If you do not have a contract follow-up, there is not any point having a contract in the first place if you are just going to put it in a drawer and never open it again."

As he illustrates ironically illustrate, the contract needs to be an active part of the process of how they manage and maintain their system, and it is a continuous process. What I2 admitted they could do to counteract this issue was:

"Our job is now to try to work a little closer to the various system owners, and to simply help them."

The IT-department for the municipalities needs to work closely with the system owners. They need to have clear communication and efficient collaboration with each other. This ensures that the system owners understand the different parts of the contracts and know what to look for when they perform the contract follow-up.

4.2.3 Evaluating vendors

One of the most crucial processes is the evaluation process of the suitable vendor for their cloud solution. If not electing the right vendor, it can quickly become costly. The evaluation processes can be performed by risk analysis, personal meetings, and how well the vendors respond to questions and are open to collaboration. At the end of the day, it is about laying trust in the vendor, and that is based on the overall impression of the vendor. This can quickly become an issue according to I3 that summarized it well:

“We like to make up our own minds based on how we perceive the vendors, so it has a lot to say to them how they appear.(..) And that is a bit of a difficult topic because you can be influenced in many ways by them, for example when we acquired such a security monitoring service and then we had a market dialogue prior to the quotation process. Then we get an impression, and then we have already formed an opinion about whether the vendor is good or not. It is basically how they appear and that has a lot to say. How our trust is in them then, and what we get in return and how good they are at answering questions.”

As it is apparent that the tender process is not only about how cheaply they can provide the service, or to what degree they can abide by the requirements they are asking for. The process is, many-sided, encompassing personal judgments, interpersonal relationships, and perceptions about the vendor's response to security requirements, among other factors. It requires a lot to perform such an analysis of vendors, which makes sense to use these parameters to assess the vendors. It also can come down to the resources of knowledge in-house of the municipalities, as I6 expressed:

“It is a bit difficult to do such due diligence and assess those vendors. If you first manage to evaluate a vendor, then perhaps you should be just as good yourself, and obviously, we are not. That's why we outsource it, and that's a problem.”

This proposes a paradox where the municipalities in the first place outsource parts of their systems because of the lack of knowledge and resource relief, but then they do not have it to evaluate or follow-up with the vendors properly. Some of the municipalities did outsource their vendor evaluation. As I3 expressed:

“When we deployed our entire infrastructure in Microsoft Azure then that time, we evaluated the vendors. We hired a law firm that assessed it at the time. I think it is not certain that the assessment would have looked the same today.”

This is to get the expertise to know whether they are in the clear legally to use it. While legal expertise can help ensure compliance with the requirements of outsourcing, outsourcing, as revealed in the literature review, comes with its own set of challenges such as cost, risk, responsibility, and more. These complexities create a compelling argument again that a centralized approach to audit would be more effective for the municipalities. This brings me to the next point which I5 expressed:

"You do not need an audit for each municipality and an audit for the company. It is not effective that every municipality performs an audit of Visma as almost every municipality is using it anyways."

This suggests that having a single comprehensive audit could potentially relieve municipalities from a lot of unnecessary audits, by streamlining the process and making it more effective for municipalities. This could potentially mitigate some of the challenges of adopting cloud solutions where a centralized instance ensures a uniform standard of evaluation of the vendors.

4.2.4 Vendor lock-in

One of the most challenging aspects of cloud solutions is vendor lock-in. Vendor lock-in refers to the difficulty in transitioning from one service to another due to compatibility issues, legal issues, and cost. Which we have seen is a common consent for adapting to new solutions. As I2 illustrated the key issues in vendor lock-in and how it applies to them:

"There are a lot of cumbersome systems that are just cumbersome to replace. (...) So if it must be replaced, then it is a massive data conversion. The employees need to undergo massive training. (...). It is a system that we have had for a long time. The barrier to replacing the systems is incredibly high, and that's a problem for us. Many of the systems are based on Microsoft servers. We use Microsoft Windows Server OS."

The statement illustrates the issue municipalities face with migration to new solutions. These systems that are talked about are important core-systems, and it is seen as too resource-demanding to replace them. The old systems can only support old standards which makes it hard to migrate them. Simply using such an old system poses a security threat as they cannot be supported by security patches etc. When municipalities are now adopting, they need to assess thoroughly so they do not find themselves in a vendor lock-in in the future. Furthermore, many of the systems are reliant on Microsoft

solutions. All municipalities expressed a concern about this issue. Many of the existing systems to the municipalities that are still not migrated to the cloud are niche systems that are required by law to have on-prem. As I5 mentioned:
"We will never get rid of on-prem because we have so much technical debt. We have many systems that were developed in the 90s that still are in use today and need to be maintained. Part of those on-prem systems we are legally required to use."

This highlights that some of the systems are almost impossible to renew or migrate to the cloud because there are not any vendors who can provide the solution. Many of the systems are technical solutions, which poses a security risk as they are considered ancient. Further, I5 mentioned that the reason vendors resist change can be:

"I think that maybe the fact that there are so few vendors actually means that they do not perhaps feel much pressure to innovate or develop."

This statement speculates that there might be a power dynamic by the vendors-client relationship, ending it that the vendors do not see any incentives to innovate or adapt to newer technology such as cloud solutions.

But there are benefits to using these large systems, as I4 mentioned:

"There is an advantage behind this, the functionality of integration of systems like the Visma financial system and the Visma school system and managing to have data flow between the two systems seamlessly. We push Visma to solve integration between their systems."

This implies that using a single vendor, like Visma, offers clear benefits, such as seamless system integration and streamlined data flow. This not only reduces the complexity of security issues for municipalities but also allows them to focus on a narrower set of potential threats, thereby enhancing security management.

As for what to do to avoid vendor lock-in, the municipalities again need to assess the vendors in the acquisition process, in the same way discussed in the "Contract Follow-up" and "security documentation" section. I1 mentions that they:

"We will at least take a credit assessment, which will be used and determined for the economy, to find out how many years they manage to stay in business. You can be unlucky with a newly started company that goes bankrupt."

This statement emphasizes the importance of a comprehensive vendor assessment in the acquisition process to mitigate the risk of vendor lock-in. One of the most important countermeasures that can be performed by municipalities. This strategic approach can significantly reduce the risk of unforeseen disruptions and vendor dependency, thereby mitigating the potential impact of vendor lock-in.

4.2.5 Security documentation from vendors

When evaluating the vendors in the tendering process and conducting the contract follow-up to get proper security documentation from the vendors is crucial. Many of the municipalities mentioned that the vendors were usually reluctant to give security documentation to the municipalities. As expressed by I5:

"Procurement can have two problems, so it's often the case that they do not expect us to ask so many questions, so the suppliers can be a bit difficult to get the information we want out of them. Perhaps, especially if you are in such a procurement situation because then things must happen quickly. So, we do not have the time to do it."

This highlights one issue they experience, and that is getting the documentation in the first place. This may be because the vendors might not feel obligated or expect to answer such demanding documentation, and it is worsened by the nature of the tender process. Furthermore, the reluctance of vendors to respond to requests for obtaining security documentation can be attributed to a transparency issue. As I6 expressed:

"I agree that we need to improve our efforts in demanding security tests and push for transparency when it comes to security testing conducted by our vendors. It is concerning that we often encounter vendors who deem the test reports as confidential company information, thus, refusing to share them with us. This situation is unfortunate. We see cases where even Microsoft and smaller vendors adopt similar practices."

This statement paints a significant gap in the vendor-client relationship when it comes to transparency around security practices, specifically security testing. The municipalities can only assess the security robustness of the cloud solution only if they have insight into these tests. The lack of transparency can be the root cause of mistrust, making it difficult for municipalities to confidently adopt these cloud solutions. This practice can go against the principle of transparency. This is essential in a vendor-client relationship, and especially in topics that concern cyber security. Another conserving behavior from the vendors expressed by some a concern about how the vendors performed security tests on their system. As I6 expressed:

"We see that very few of the vendors dare to document security tests. It scares us a little. Yes, that is probably the worst. There is a bit of a poor security focus, a lot of mistakes that are repeated, and especially the issue of identity management is probably the worst part."

What this statement expresses are a concern with the vendors' practices of performing security tests and documenting them. The reason they might not dare to do it is because of their reputation. This issue is a paradox where the vendors are reluctant to perform testing because of the reputational damage as they may seem less secure, but not doing it will make the security issues not addressed in the first place. Without these security documents, the municipalities cannot assess the security of the proposed cloud solutions.

What municipalities can do to mitigate this issue may lay in the tender process. As indicated by I6:

"We ask them several critical questions in the tender process which they must respond to. If you ask questions about redundancy and other things, and that is what we can emphasize as quality, as it says in the tender, it is about how they respond to this."

What this comment emphasizes is that asking comprehensive and critical questions can reveal the quality of the cloud solutions that are offered by the vendors. Not only do the answers themselves reveal the quality of the security, but it also provides tangible evidence of their competence. Therefore, in the tendering process, it is often wise to use time and ask the right questions that will aid the municipality to ensure the selection of the vendor is the highest quality provider.

4.3 Legal and Regulatory Considerations

4.3.1 Legal aspects

What makes the adoption of cloud solutions challenging for many municipalities are the legal issues that arise from it. The complexity arises from conflicting laws, as the data is stored and processed in foreign countries or falls under the jurisdiction of foreign legal systems. Managing and ensuring compliance with these regulations requires significant resources. All the municipalities expressed this as a problem. I2 stated that:

"It is insanely resource-intensive to deal with all the laws and regulations. I believe that this is the biggest obstacle to digitization and innovation."

An example pointed out by I4 stated that:

"Due to legislation, which we have a lot of in Norway, especially of what is worthy of archiving should be in Norway. Many municipalities use Office 365, and it is stored in Europe. We have our data centers in Ireland and the Netherlands."

What this statement highlights are the Norwegian Archives Act, which states that "It is prohibited to take public archives out of Norway (export)" (The Archives Act, 1992, § 9-b). This law almost makes it impossible to store data outside of the boundary of Norway. As mentioned, I4 highlights how the new Schrems II judgment has even made it even more complex for municipalities:

"When the Schrems II judgment was issued. There was a perception that moving everything back to on-premises was the only viable option, even though it was an exaggeration. It is not completely doable to abide by it, everyone breaks the law today if you ask me."

This has made it even more problematic and more relevant for the discussion on transferring data across borders. Several others think they somewhat broke the law, but indeed see no other option. What the municipalities do is assess the risk of placing the data outside the organization and weigh the importance of placing the system up to the cloud. GDPR has created a consistent and legal framework for such issues, but there are downsides to it. Several of the municipalities mentioned it as problematic. As I2 mentioned:

"It is clear that GDPR is the biggest challenge, and the one that I say on a daily basis is up for discussion. In every new system, every change in every innovation idea, the GDPR very often touches it."

As I2 illustrates, the GDPR is quite comprehensive, rigid, and it requires a lot of resources to be compliant with it. Also, what makes it important to be compliant with the GDPR is the potentially large fine one could get from breaking it. As we have seen the Norwegian laws can to a degree be violated, but the GDPR makes it infeasible to be in sort of a gray area of the law. At the end of the day, the departments need their systems so municipalities cannot always be on the right side of the law. As I3 said:

"And thus, we end up sometimes doing things that may be on the border of what is not completely legal. The municipality must function as well, and we must have systems that function and are secure. Sometimes you have no alternative solution for the systems."

These regulations are there for a reason and that is mainly to protect user privacy or as the more local laws ensure that the cloud solutions are secure. Therefore, it is not ideal that municipalities take shortcuts and choose to prioritize functionality rather than security or privacy. What I5 argued is that:

"Microsoft has armed guards and there is extreme security from a technical standpoint. You could argue that a Norwegian data center is less secure from that perspective. But from a Max Schrems perspective, the USA is a country with fewer privacy rights compared to the EU, but still, I do not think it is such a big risk. Then we are a bit lucky that we are perhaps "friends" with the USA. Not everyone is."

It highlights the practical choices available to municipalities, as one can prioritize privacy to a great extent. However, the potential risks might be minimal compared to the advantages the systems give. What is necessary is the implementation of revised laws that are aligned with the practical reality, as mentioned by I2:

"The South-Eastern Norway Regional Health Authority was going to push some patient data out into Microsoft Azure infrastructure. I think it was last week. It was sort of against all recommendations. I think it is good that they did it, because it helps to challenge the existing regulations."

Municipalities can put pressure on the government by taking daring actions, such as the example of one municipality and the South-Eastern Norway Regional Health Authority storing sensitive data on Microsoft servers. This can serve as an accelerator for discussions within departments and the legislative authority, making it a relevant and timely topic for consideration and potential policy changes.

4.4 Supply Chain Management

4.4.1 Supply chain issues

One of the biggest security concerns regarding cloud solutions in Norwegian municipalities that was discussed during the interviews was supply chain issues. Almost all the informants thought that they had been subject to a supply chain attack, where "Nordkart" was mostly the culprit. Such attacks make the municipalities worried, and they understand the issue that they need to trust the vendor they have control of their data. As I2 expressed:

"When others maintain and produce systems for us, they are the ones who store and process our data. They are the ones who have our solutions, so we do not have our hands on the wheel anymore. Having good contracts and agreements is fine, but at the same time, you also must trust that the supplier does its job. We are a bit worried about supply chain attacks because we do not have full control."

This suggests that the municipalities must rely on trust, and as mentioned earlier the resources available to perform due diligence on the vendors and the sub-vendors simply are not there. This is a security issue, as there is no way of checking if the vendors have control of their sub-vendors, and this even worsens as the vendors must do the same and rely on trust in the sub-vendors, which gets fuzzier for each joint down the supply chain. This presents a larger attack surface of the cloud solutions and increases the security issues etc. These issues make every aspect of the security management hard for the municipalities to assure is well maintained. As I3 mentioned:

"When we have bought cloud solutions, we really have no control. The only thing we have is the login part that goes into our environment, so that they log in with this type of single sign-on, so it is connected to us. But beyond that, we have very little control over the system and the security."

As this illustrates the actual accessibility to security mechanisms can be limited, and the security relies on the vendors as they provide the cloud solution. It is evident that the accessibility to security mechanisms can be limited, and there is an underlying dependency on vendors providing cloud solutions. The responsibility does not fall in the hands of one vendor but is shared among them down the supply chain. Municipalities do not have that much access to the sub-vendors as expressed by I3:

"What we often lack the ability to thoroughly evaluate is the extent of access and oversight we have over their sub-vendors."

Municipalities do not get the opportunity to assess them to a large extent, yet they can have a significant impact on the overall security landscape. The access can either be to business secrets, or reluctance in cooperating as it can be resource-consuming to answer municipalities for the sub-contractors.

4.5 Technical Considerations

4.5.1 Authentication

A significant authentication challenge that emerged from the interviews was the struggle with implementing Single Sign-On (SSO) in municipalities that adopt cloud solutions. The issue, although technical, has broader implications on security and user management, and was a concern shared by most of the interviewees. I2, for instance, underscored their difficulty stating:

"Our challenge is to achieve single sign-on in fully integrated across the systems. We have not achieved it yet that well."

This remark highlights the intricacies of ensuring seamless authentication across different cloud solutions, and it is clear in a dynamic environment of a municipality. The struggle is not just technical implementation of identity management but also raises a substantial security concern. I5 quoted that:

"How do we secure it when everyone can access all the data from anywhere?"

It raises one of the core security challenges associated with cloud adoption. That is ensuring secure and controlled data access, is a much more different environment compared to on-prem solutions that are within the organizational boundary. Identity management has become more and more widely used such as Firewalls, 2-FA, and Zero-trust management, which all the municipalities aim to implement in the systems. The reality of how identity management is in the cloud solutions to the municipalities are varying in quality. As stated by I6:

“One of the things we often see with clouds is that identity management is very poor. We see a lot of identity problems.”

The quote expresses concern about identity management, and it paints a picture that it is a common problem that vendors do not prioritize identity management. What municipalities have adopted recently are integrated solutions that offer federation[4], and the most common solution that municipalities use is Microsoft Active Directory. As I6 described, they demand federation in the procurement requirements. As they stated:

"Yes, in our procurement requirements, we want federation. This means that we control the user accounts delivered by the SaaS service providers to us."

Getting solutions such as Microsoft Active Directory gives the municipalities more power to configure and tweak how they manage their users, rather than the vendor.

4.5.2 Availability

One of the key concerns that emerge from adopting cloud solutions is the question of availability. Based on the systems of the municipalities Availability is crucial in certain systems and can be a catastrophe if there is downtime to the systems. The municipalities showed concern about unforeseen circumstances. As expressed by I2:

"We have a cloud-first approach, but we must evaluate its availability. The advantage of having a patient journal system locally is that if network lines disappear or something happens like the power going out in the entire district, we can keep the system operational."

The power outage scenario was described by several and emphasizes the need for contingency plans when network error or power outages occur, a concern voiced by I4:

"The right balance is crucial when evaluating services. For instance, we need to consider the level of uptime we can expect in the event of a line break or loss of connectivity to the outside world, especially when our storage system relies on cloud solutions."

[4] "Federation is a collection of domains that have established trust" (Microsoft, 2023).

As it is apparent losing availability to cloud solutions if they are placed in the cloud, the municipalities have no way of accessing their data or the systems may fail to function properly. In one of the municipalities, there was an issue where a digital app used to unlock doors stopped functioning for elderly individuals receiving home nursing care. Two personal alarms[5] were triggered, but fortunately no one was hurt during the incident. This illustrates that such instances can in the worst-case lead to death.

On the other hand, the interviews revealed concerns about the reliability of the cloud service providers. I3 expressed that there while there are cost benefits to cloud services, The reliability of the large vendors is a significant factor for their adoption:

"The cost is lower, and opting for a solution like Microsoft offers advantages due to their size and commitment to maintaining system stability."

As the scenario of losing the availability of the service providers, the municipalities expressed a concern of redundancy in the cloud providers. As expressed by I6:

"While most providers demonstrate they are good at handling personal data in addition to other aspects. Although we see there is the lack of redundancy in the data center they have selected. If you get an unfortunate scenario like in Germany, where the data center burned down, then you do not have that data anywhere else."

Many of the municipalities did indeed have hybrid solutions as a failsafe for the most critical systems but said that they did not have any backup of the systems that ran as a cloud solution.

What municipalities do for the availability issue is an assessment of the criticality of the system. As I4 expressed:

"We must make the assessment. There is a real challenge that network lines can be down. There can be a DDoS attack against us. We cannot trust the internet alone."

[5] Elderly individuals have the option of wearing a wristwatch equipped with an emergency button that can be pressed in case of incidents such as falling over, enabling them to call for immediate assistance.

If it is too big of a risk for the system, the solution can simply not be on a cloud solution. If they do, there should be redundancy mechanisms like backup and local systems that work as a fail-safe in case of a halt in the continuity. This is proven to be costly or resource demanding.

4.5.3 Confidentiality

Municipalities store and process sensitive data and as more sensitive data is stored and processed in the cloud, maintaining confidentiality becomes increasingly critical. I3 emphasized the criticality of data confidentiality, in relation to sensitive data:

"It is almost worse if the data comes into the wrong hands. We have a lot of sensitive data in it. These are journal systems that contain a lot of information about the citizens. (...). If the data disappears, it is clearly more critical."

As for how they deal with the issue of data leakage or confidentiality breach, I6 pointed out that they use encryption to make sure no unwanted party could access their data:

"We encrypt our physical machines. If it disappears in transit, we encrypt our data, and we encrypt our backups."

Confidentiality is a concern for municipalities. Handling sensitive data requires careful consideration and robust security measures to ensure confidentiality. In the "Authentication" and "Multi-tenancy security problems" Chapter elaborates more about the importance of authorization to keep confidentiality. As for encryption and assessing the risk of the vendors and systems that they are going to use can counteract this issue to adapt to cloud solutions.

4.5.4 Multi-tenancy security problems

Municipalities have highlighted multi-tenancy as a significant issue in the context of cloud solutions, particularly with respect to data isolation and cyber security. Multi-tenancy was seen by all the municipalities as a threat whereas I6 expressed:

“Yes, it would be very unfortunate if you logged in and saw data from another municipality, so that is something we always ask about how they ensure to separate their customers.”

This apprehension highlights the core issues of multi-tenancy, where the vendors must ensure data isolation as there typically are several municipalities' data stored and processed on the same hardware. The municipalities recognized that their data centers offer a certain level of security due to the physical barriers, but also recognized the potential exposure when using cloud services.

I6’s case expressed that they were suspicious of potential security flaws or architectural design flaws, where it was possible for either them or other municipalities to access each other's data. They expressed:

“We suspect it based on how we see the architecture design. (...). We understand that it is probably possible in some places based on the current architecture."

On that basis, the vendors and municipalities need to be aware of this problem. As all the municipalities recognized this as a potential problem, half of them said it was not discussed within their organization. What we can draw from these interviews is the need for robust data isolation strategies by the vendors of cloud solutions. Vendors must be proactive and provide assurance and show consistent data isolation strategies, while the municipalities need to be proactive in the process demanding or requiring them to ensure there is not any data exposure due to multi-tenancy issues.

Table 3 Overview of the empirical findings

Theme	Issues	Description	Mitigation Strategies
Organizational challenges	User compliance	Municipalities experience user compliance issues, such as password reuse leading to security breaches and the mishandling of sensitive data on platforms that store data abroad like Microsoft Teams, in violation of the archival law.	Continuous security awareness training is crucial to mitigate these issues, emphasizing unique password usage and compliance to data handling policies. This continuous awareness effort should improve policy compliance and mitigate potential data leaks.
	Collaboratio n	Small municipalities can benefit from collaboration with larger municipalities, but it can slow innovation. Posing a risk of using legacy systems.	Collaboration and balancing it with individual decisions could speed innovation which in the end improves security. Collaborative projects often have access to greater resources, enabling them to implement robust measures that facilitate the migration of highly sensitive systems to the cloud.
	Conflict of interest	Project owners, often lacking IT-competence, prioritize functionality over security, sometimes even excluding IT-departments from the evaluation of cloud solutions. As a result, systems with weak security or potential data privacy violations can be integrated. This situation is further complicated by organizational structure, as IT-departments can be seen as external entities,	Better collaboration and communication between project owners and IT-departments is essential. By involving IT professionals early in the decision-making process, security and technical aspects of systems can be properly assessed. Additionally, organizations should reconsider their structure to bridge any perceived gaps between project owners and IT departments. Enhancing the role of IT departments in system acquisition could prevent potential security risks and facilitate compliance with data protection regulations.

Theme	Issues	Description	Mitigation Strategies
		and a lack of proactive communication with the Privacy Commissioner.	
	Executive Involvement in Cloud Security Adoption	The adoption of secure cloud systems in municipalities are dependent on the involvement and understanding of the management towards digitalization and security. An executive who is disconnected and uninformed about IT-related matters can blindly approve measures or propose abstract strategies like "cloud-first" without understanding the costs or risks involved, potentially leading to ineffective digitalization and increased security issues.	Executives should be more involved and educated about cloud adoption security. Clear, well-informed strategies should replace abstract ones, with a deep understanding of the costs and risks associated with cloud solutions. This executive involvement can then spread a culture of security throughout the organization, promoting more successful and secure cloud adoption.
	Resources	Adoption of cloud solutions requires significant resources for migration and employee training. This challenge is further complicated by the political landscape of municipalities, where budget decisions can be influenced by non-technical decision-makers who may prioritize cost	Hiring external consultants can relieve the issues, despite the higher cost, could provide expertise in adapting to cloud solutions. Also, adopting cloud solutions can free IT-departments from the burden of system operation, enabling them to focus more on security and strategic consulting within the organization. Hence, effective resource allocation and increasing political will towards prioritizing security can aid in successful and secure cloud adoption.

Theme	Issues	Description	Mitigation Strategies
		and functionality over security.	
Environmental issues	Guidelines, strategies, and Frameworks	Municipalities find the guidelines to be too numerous, vague, and difficult to find, complicating cloud solutions' implementation. Conflicting directives from different authorities further escalated the problem, leading to potential legal risks and inconsistent security measures.	The informants expressed a need for clear, unified guidance, ideally issued centrally to aid decision-making and relieve the municipalities' assessment burden. A voluntary organization, KiNS, has made efforts in providing a uniform framework for adopting cloud solutions, indicating a move towards reducing bureaucratic barriers.
	Contract follow-up	In municipalities, contract follow-ups after implementing cloud solutions often fall on system owners, who may lack the required competence. This situation can lead to non-compliance from the vendors with the agreements, posing a security risk.	IT-departments in municipalities should work closely with system owners. Through clear communication and collaboration, they can help system owners understand contract details, enabling them to effectively manage and maintain their systems.
	Evaluating vendors	Evaluating vendors for their cloud solution is a resource-intensive process for the municipalities. This process involves not only assessing the cost and	Centralizing the evaluation process could increase efficiency and reduce unnecessary redundancies. A centralized instance could ensure a uniform standard for evaluating vendors and provide more through evaluations, relieving municipalities of this burden.

Theme	Issues	Description	Mitigation Strategies
		technical requirements but also the overall impression of the vendor, potentially laying a great deal of trust in the vendor. However, municipalities often lack the necessary expertise and resources to effectively evaluate vendors. Furthermore, the current process involves a high degree of redundancy with each municipality independently auditing the same vendors.	
	Vendor lock-in	Vendor lock-in is due to compatibility issues, costs, legal issues, and old systems that are difficult to replace. These barriers are compounded by the fact that municipalities often rely on old, niche systems that are legally required or have been in place for a long time. If these systems are not updated or replaced, they could pose a significant security risk. Additionally, a lack of competition among vendors might reduce the vendors incentives to innovate and adapt to	To mitigate the risk of vendor lock-in, municipalities need to carefully assess vendors during the acquisition process. The evaluation should include an assessment of the business financial stability to foresee that the vendor will go bankrupt. Also, the assessment should consist of compatibility of solutions with existing systems Utilizing a single vendor for multiple systems can also have benefits, such as seamless integration and streamlined data flow, which can reduce security risks and simplify security management.

Theme	Issues	Description	Mitigation Strategies
		newer technology such as cloud solutions.	
	Security documentation from vendors	Obtaining adequate security documentation from vendors during the tendering process has shown to be a persistent issue. The vendors often do not expect detailed inquiries and might be reluctant to provide in-depth security information. Additionally, there seems to be a transparency issue, with vendors often unwilling to share security test results, arguing that it is confidentiality of company information. This lack of transparency and insight into the security robustness of the cloud solution can breed mistrust and hinder the adoption of cloud solutions.	Municipalities could use the tender process as an opportunity to ask critical questions to the vendors. The answers to these questions can reveal the quality of the cloud solutions offered by the vendors and provide evidence of their competence. Additionally, municipalities can emphasize the importance of transparency and thorough security testing in their discussions with potential vendors. By doing so, they could make vendors more open about their security practices. This can lead to more informed decisions in the selection process.
Legal aspects	Legal aspects	Municipalities face legal challenges with cloud adoption due to conflicting national and international laws on data storage and processing. Laws like Norway's Archives Act, GDPR, and the Schrems II ruling. This makes it	To deal with these legal issues, municipalities should thoroughly understand the regulations, assess data storage risks, and prioritize system security and privacy. By pushing boundaries and engaging in daring actions, for example storing sensitive data on foreign servers, they could pressure legislators to revise existing laws in line with practical cloud computing realities.

Theme	Issues	Description	Mitigation Strategies
		resource-intensive to ensure compliance.	
Supply Chain Management	Supply chain issues	The primary issue lies in the dependency on vendors and sub-vendors who maintain and process the municipalities' data. The municipalities often lack control over the security of their data and systems since they are in the hands of the vendors. They also have limited resources to perform due diligence on the vendors and their sub-vendors. This results in a large attack surface and an increase in security risks.	Having good contracts and agreements can help mitigate these security risks, although they are insufficient alone. However, they face challenges in assessing the security practices of the sub-vendors due to limited access and cooperation. This highlights the need for more resources and capabilities to monitor, evaluate, and ensure the compliance of sub-vendors with security requirements.
Technical Considerations	Authenticati on	Implementing Single Sign-On (SSO) across all systems is a significant challenge faced by municipalities adopting cloud solutions. This challenge has both technical and security implications, with one of the main security concerns being the control of data access. Furthermore, the quality of identity management within cloud solutions has been found to vary, often poorly	municipalities are focusing on implementing identity management techniques such as Firewalls, 2-Factor Authentication (2FA), and Zero-Trust Management. Furthermore, municipalities are seeking integrated solutions that offer federation, such as Microsoft Active Directory. By integrating such solutions, municipalities gain more control over user management, providing a stronger control in securing their data and systems. The specification of federation in the procurement requirements is a strategy being adopted to maintain control over user accounts.

Theme	Issues	Description	Mitigation Strategies
		prioritized by vendors, leading to additional difficulties for municipalities.	
	Availability	The availability and reliability of cloud solutions, especially during network or power outages can become an issue. Critical systems' downtime can lead to severe consequences. The lack of data center redundancy and local system backups worsen these risks.	Municipalities must evaluate system criticality to determine if a cloud solution is appropriate. For high-risk systems, redundancy mechanisms like local backups or fail-safe systems should be considered, despite their costs.
	Confidentiality	Sensitive data is stored and processed in the cloud. Municipalities have expressed concerns about maintaining data confidentiality. Breaches or data leaks could result in severe consequences.	Municipalities utilize encryption for physical machines, data, and backups to ensure data confidentiality and protect against unwanted access. Risk assessments of vendors and systems are also carried out to reinforce data confidentiality in cloud solutions. Lastly, the issue of authorization measures is important to hinder unauthorized access.
	Multi-tenancy security problems	The adoption of cloud solutions brings forward concerns about multi-tenancy and data isolation. The municipalities fear that their data might become accessible to unauthorized actors due to potential architectural design flaws in multi-tenant environments.	Both vendors and municipalities need to ensure robust data isolation strategies. Vendors should provide assurance through consistent data isolation plans, and municipalities must proactively demand or require these safeguards to mitigate potential data exposure risks.

5 DISCUSSION

Based on the key findings presented, the results align with the literature and support the hypotheses that the adoption of cloud solutions by municipalities brings about various organizational challenges and considerations.

The empirical findings highlight user compliance issues, such as password reuse and mishandling sensitive data, which are common challenges in digital environments. In line with the literature, there is strong support that continuously performing security awareness training can mitigate such issues (Pai & Basu, 2007. P. 31). Thus, municipalities should keep working and improving their security awareness.

The empirical findings also emphasize the importance of collaboration between municipalities, particularly for small ones, to benefit from innovation. Collaboration can both enhance innovation and pose challenges that need to be balanced. For instance, collaboration can slow innovation, resulting in vulnerable old systems. The literature did not address such issues directly. However, it emphasized collaborating internally with the management's involvement (Nakatsu & Iacovu, 2009, p. 58; Tafti, 2005, p. 555). The issue seems to be the same: lack of qualification and knowledge (Nakatsu & Iacovu, 2009, p.62). The mitigation technique for collaboration that hinders innovation could be to improve mutual understanding and collaboration (Hansen et al., 2011, p. 183).

The literature underscores the critical role of executive involvement and understanding of security in successful cloud adoption. The critical role of executive involvement aligns with the recurring theme in numerous studies, where a lack of managerial involvement often results in project derailment (Nakatsu & Iacovu, 2009, p. 58; Tafti, 2005, p. 555). Moreover, empirical findings and academic studies pinpoint a critical concern: the qualifications and knowledge of those at the helm (Nakatsu & Iacovu, 2009, p. 62).

Another critical issue is the conflict of interest, where project owners prioritize functionality over security. This pattern reveals a widespread disregard for security considerations in the decision-making process. The root of this issue may lie in managerial disengagement. The empirical findings highlight the need for better collaboration and involvement of IT-departments in evaluating cloud solutions to ensure proper security assessment. Hansen et al. proposed a model that facilitates mutual understanding and collaboration, thereby aligning IT-managers and system-owners, thus mitigating these issues that come with the lack of executive involvement (Hansen et al., 2011, p. 183).

The empirical findings regarding resource allocation and the influence of non-technical decision-makers on budget decisions also align with expectations that resources play a significant role in successful cloud adoption. This factor again lands on the management's roles and responsibilities. The lack of knowledge from the management can lead to a down prioritization of the security of the solution, thus ensuring the managers have the knowledge and mutual understanding that is in line with the IT-department (Hansen et al., 2011, p. 183).

Regarding the environmental issues, the findings indicate challenges with guidelines, strategies, and framework are in line with the literature that both clearly states that the vague and inconsistent strategies have led the adoption of cloud solution not only slow but it has affected security (Scholtz et al., 2016; KMD, 2015, p. 25). The vague guidelines align with KMDs literature which is set in the same context as this thesis which is Norwegian public organizations. Therefore, empirical data and the literature emphasize the need for more unified and clear guidelines, strategies, and frameworks (KMD, 2015, p.16). Clear guidelines can mitigate the issue raised by municipalities regarding the resource-demanding process of performing vendor evaluations. Furthermore, such guidelines can streamline the due diligence process and reduce exposure to technical risks.

Clear guidelines can mitigate the issue pointed out by the municipalities, which was that evaluating vendors was resource-intensive, and centralizing the evaluation process can lead to regaining control of the supply chain. However, the municipalities admitted to the lack of competence in contract follow-ups. These challenges were anticipated, and the recommendations for clear and unified guidance and closer collaboration between IT-departments and system owners.

The same applies to the legal issues that municipalities face during cloud adoption. Both the literature and empirical data agree that data that cross jurisdictional zones become problematic (Ghaffar, 2020; Nakatsu & Iacovou, 2009, p. 64; Pai & Basu, 2007; Nassimbeni et al., 2012, p. 408). There is a clear need for revised and unified laws at several levels from local jurisdictions and international legislators (Scholtz et al., 2016, p. 11). The municipalities desired a more proactive approach, proposing that they push boundaries and undertake bold actions to prompt legislative authorities to formulate new laws and guidelines. This underscores the pressing need for clear regulations governing municipalities and suggests that they might need to take matters into their own hands to catalyze change.

The supply chain issues described in the empirical data are one of the root causes of many challenges. It can be described as a loss of control down the supply chain. The literature was clear that when municipalities adopt cloud solutions, they reduce the control over data storage and processing (Pearson & Benmaeur, 2010; Hamlen & Thuraisingham, 2012, p. 2; Xiao & Xiao, 2012, p. 883). What the empirical data suggest is that the opportunity to perform due diligence is impaired due to resources such as cost and knowledge. The literature described that due diligence is essential to circumvent pitfalls in the cloud adoption process (Pai & Basu, 2007, p. 29). However, the literature identified that due diligence made it hard as the limited access of the vendors makes it increasingly challenging to perform due diligence (Bachlechner et al., 2013, p.44; Kshetri, 2013, p. 379). This was reflected in the municipalities as they found it challenging to access security documentation from the vendors or found themselves in vendor lock-in due to no willingness or incentive to innovate. According to the literature, municipalities should pressure vendors to be more open and continue to use collaboration efforts to relive resources (Pai & Basu, 2007, p. 31; Ksheri, 2013, p. 379; KMD, 2015, p. 31). The municipalities admitted they needed to pressure vendors more but utilized various collaboration means to mitigate this issue.

Municipalities face challenges in authentication management. The literature explains this as a leading confidentiality breach (Khidzir et al., 2010, p.197; KMD, 2015, p. 15; Pai & Basu, 2007, p.31). The lack of this could lead to a domino effect that puts municipalities at risk, such as maintaining data confidentiality, addressing multi-tenancy security problems, and data isolation. All these issues were well addressed in the literature and empirical data. What municipalities can do to protect the confidentiality of the cloud solution is; Identity management techniques, encryption, risk assessments, and demand for data isolation strategies. In addition, the literature revealed that comprehensive SLA and contracts could ensure that the vendors meet up to those requirements of confidentiality agreed upon (Almutairi & Riddle, 2018, p. 45; Ali & Osmanaj, 2020, p. 10).

Availability issues were also considered a key concern in the literature and the empirical findings. Redundancy in its system, such as backup, was empathized by the municipalities which the literature reveals the same mitigation technique (Hamlen & Thuraisngham, 2013, p. 3; KMD, 2015, p. 11; Kyriakou et al., 2020, p. 249; Pearson & Benameur, 2010, p. 694).

The key findings regarding organizational challenges are user compliance, collaboration, conflict of interest, executive involvement, resources, environmental issues, legal and regulatory considerations, supply chain management, due diligence, authentication, and availability. Municipalities' adoption of cloud solutions supports the literature, highlighting the complex nature of cloud adoption and the need for careful consideration of various factors. Some are more important than other as it is root causes.

5.1 Limitations & Further Research

This section will address the limitations regarding the thesis and the future research direction to gain an even better understanding of security issues in cloud adaptation for Norwegian municipalities.

The fact that this thesis was written by one person has in fact impacted its comprehensiveness of this thesis. This has reduced the opportunity for discussions and insights that could have been gained if the thesis was done collaboratively with other peers. Fortunately, the guidance and insights provided by my supervisor have been invaluable, helping to mitigate these limitations to some extent.

One of the limitations of my thesis was the sample of the municipalities that were interviewed, which might not be representative of all municipalities, many of the municipalities were medium-sized, and one was small. If I had the opportunity to have a larger sample size, I would be able to get a more nuanced image of how municipalities experience the process of adopting cloud solutions and what security-related issues they experience.

The nature of the research design which consisted of a qualitative approach, one could argue that the confidence of the findings is weaker compared to if it would have been conducted a quantitative approach. It would be interesting to further confirm my findings in a larger sample in a form of quantitative approach to confirm the findings.

The diverse range of options that are offered by cloud providers has not been in focus when it comes to differentiating between them. For example, solutions that are IaaS can be more likely to have security challenges compared to SaaS solutions as it places more parts of the system outside the organizational boundary. Therefore, it would be interesting to further dig into the differences depending on the deployment solutions.

Secondly, the reliance on the reported experiences was based on different experiences and perceptions of people, which might not fully reflect the issue's complexity or be representative to all municipalities. Further, the issues were not explored directly with the systems or the security measures that were implemented. Thus, the reliability of the data depends on reported information and may not reflect the actual state of the solutions. .

This thesis has explored in depth the security issues as well as mitigations of cloud adoption in a public context, which create a foundation for some aspects of cloud adoption.

6 CONCLUSION

We can conclude that Norwegian municipalities meet many challenges or barriers when they adopt systems that run on cloud solutions. Based on my research by the interviews and the literature review that was performed, many of the factors or barriers of the literature review states apply in the context of Norwegian municipalities. The overall impression left by the interviewees is that the barriers identified are large and complex but can be counteracted with governmental initiatives and improved processes of allocation of resources throughout the whole life cycle of the system.

The provided findings shed light on the organizational challenges faced by municipalities in cloud adoption. It emphasizes the importance of continuous security awareness training for improving user compliance, the potential risks and complexities associated with collaboration with larger municipalities, the necessity of executive involvement and understanding of digitalization and security.

By considering alternative explanations and evaluating the significance of these challenges, we can argue for the validity of the literature and Empirical findings. The findings highlight the need for effective training programs to address user compliance challenges. Collaboration with larger municipalities is identified as a potential risk due to legacy systems and divergent interests, underscoring its impact on innovation and security outcomes. The findings stress the importance of executive involvement in digitalization and security, emphasizing their direct influence on cloud adoption success. Furthermore, the legal and governance aspect emphasizes that higher instances need to initiate and come with clear and strategies and legal frameworks. Lastly the technical issues are related primarily to confidentiality and availability issues, making it important that vendors comply according to the agreements.

Overall, the findings provide valuable insights into the organizational challenges faced by municipalities in cloud adoption. It underscores the need for targeted training programs, cautious collaboration, strong executive support, and careful assessment of vendors as well as the need for initiative by higher powers. By taking these factors into account, municipalities can navigate the challenges associated with cloud adoption more effectively, fostering secure and innovative digital transformations.

7 BIBLIOGRAPHY

Abd Al Ghaffar H.-t.N. (2020) "Government Cloud Computing and National Security" Review of Economics and Political Science Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/REPS-09-2019-0125

Abdullah L. & Quintero J. (2019) "Sealed computation: a mechanism to support privacy-aware trustworthy cloud service" Information and Computer Security Vol. 27 No. 5 pp. 601-620. https://doi.org/10.1108/ICS-11-2018-0133

Ali O. & Osmanaj V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. Computer Law & Security Review 36 105396. https://doi.org/10.1016/j.clsr.2020.105396.

Almutairi M. & Riddle S. (2018). State of the art of IT outsourcing and future needs for managing its security risks. In 2018 International Conference on Information Management and Processing (ICIMP) (pp. 42-48). London UK: IEEE. https://doi.org/10.1109/ICIMP1.2018.8325839

Bachlechner D. Thalmann S. & Maier R. (2013). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. Computers & Security 40 38-59. https://doi.org/10.1016/j.cose.2013.11.002

Bennet, N. & Lemoine, J. (2014, January 1). What VUCA Really Means for You. Harvard Business Review. Retrieved from: https://hbr.org/2014/01/what-vuca-really-means-for-you

Bhatti B. M. Mubarak S. & Nagalingam S. (2021). Information Security Risk Management in IT Outsourcing – A Quarter-century Systematic Literature Review. Journal of Global Information Technology Management 24(4) 259-298. https://doi.org/10.1080/1097198X.2021.1993725

Braun V. & Clarke V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology 3(2) 77-101. doi:10.1191/1478088706qp063oa

Creswell, J.W. (2014). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 5th ed. Upper Saddle River, NJ: Pearson Education.

Dhillon G. Syed R. & de Sá-Soares F. (2016). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. Information & Management 54(4) 452-464. https://doi.org/10.1016/j.im.2016.10.002

Digdir (2020) Hva er Schrems II-dommen Retrieved from: https://www.digdir.no/handlingsplanen/hva-er-schrems-ii-dommen/2581

Gates S. (2002) Review of methodology of quantitative reviews using meta-analysis in ecology. Journal of Animal Ecology 71: 547-557. https://doi.org/10.1046/j.13652656.2002.00634.x

Grady M. P. (1998). Qualitative and action research: A practitioner handbook. Phi Delta Kappa International. Retrieved from: https://books.google.no/books?id=JOr3-A3-LbwC&lpg=PA1&ots=hC_OO8jFP5&lr&hl=no&pg=PA1#v=onepage&q&f=false

Hamlen K. W. & Thuraisingham B. (2013). Data security services solutions and standards for outsourcing. Computer Standards & Interfaces 35(1) 1-5. https://doi.org/10.1016/j.csi.2012.02.001

Hansen A. M. Kraemmergaard P. & Mathiassen L. (2011). Rapid Adaptation in Digital Transformation: A Participatory Process for Engaging IS and Business

Leaders. MIS Quarterly Executive 10(4) Article 5. Retrieved from: https://aisel.aisnet.org/misqe/vol10/iss4/5

Jamshed S. (2014 5th September). Qualitative research method-interviewing and observation. J Basic Clin Pharm. .87-8. doi: 10.4103/0976-0105.141942.
Johannesson P. Perjons E. (2014). An Introduction to Design Science. Springer. ISBN: 978-3-319-10632-8

Kajiyama T. Jennex M. & Theophilus A. (2017). To cloud or not to cloud. 25(5) 624-659. https://doi.org/10.1108/ICS-07-2016-0051

Kallio H. Pietilä A. M. Johnson M. & Kangasniemi M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of advanced nursing 72(12) 2954-2965. https://doi.org/10.1111/jan.13031

Khalfan A. M. (2004). Information security considerations in IS/IT outsourcing projects: A descriptive case study of two sectors. International Journal of Information Management 24(1) 29-42.https://doi.org/10.1016/j.ijinfomgt.2003.12.001

Khidzir N. Z. Mohamed A. & Arshad N. H. (2010). Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. In 2010 International Conference on Information Retrieval & Knowledge Management (pp. 194-199). Shah Alam Malaysia. doi:10.1109/INFRKM.2010.5466918

Kitchenham B. & Charters S. (2007). Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3. Keele University and University of Durham Technical report EBSE-2007-01. https://doi.org/10.1145/2372233.2372235

Kshetri N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy 37(4–5) 372-386. Retrieved from: https://doi.org/10.1016/j.telpol.2012.04.011

Kyriakou N. Euripides L. & Paraskevi D. (2020). Factors affecting cloud storage adoption by Greek municipalities. In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance (pp. 244-253). ICEGOV '20. Retrieved from: https://doi.org/10.1145/3428502.3428537

Lincoln Y. S. & Guba E. G. (1985). Naturalistic inquiry. Newbury Park CA: Sage Publications.

Microsoft (2023) What is federation with Azure AD? Retrieved from: https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/whatis-fed

Miles M. B. & Huberman M. (1994). Qualitative Data Analysis (2nd ed.). Sage.

Mvelase, P., Dlodlo, N., Williams, Q., & Adigun, M. (2011). Virtual Enterprise Model for Enabling Cloud Computing for SMMEs. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications (ISWSA '11) (pp. 1-6). Amman, Jordan: Association for Computing Machinery. doi:10.1145/1980822.1980835

Nakatsu R. T. & Iacovou C. L. (2009). A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study. Information & Management 46(1) 57-68. doi: 10.1016/j.im.2008.11.005.

Nassimbeni G. Sartor M. & Dus D. (2012) "Security risks in service offshoring and outsourcing" Industrial Management & Data Systems Vol. 112 No. 3 pp. 405-440. https://doi.org/10.1108/02635571211210059

Okoli C. & Schabram K. (2012). A Guide to Conducting a Systematic Literature Review of Information Systems Research. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1954824

Pai A.K. and Basu S. (2007) "Offshore technology outsourcing: overview of management and legal issues" Business Process Management Journal Vol. 13 No. 1 pp. 21-46. https://doi.org/10.1108/14637150710721113

Paré G. Trudel M.C. Jaana M. & Kitsiou S. (2015). Synthesizing Information Systems Knowledge: A Typology of Literature Reviews. Information & Management 52:183–99. URL: https://doi.org/10.1016/j.im.2014.08.008

Pearson S. & Benameur A. (2010). Privacy Security and Trust Issues Arising from Cloud Computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). Indianapolis IN USA. doi: 10.1109/CloudCom.2010.66

Polyviou A. & Pouloudi N. (2015). Understanding Cloud Adoption Decisions in the Public Sector. 48th Hawaii International Conference on System Sciences 2015 pp. 2085-2094 https://doi.org/10.1109/HICSS.2015.250

Recker J. (2021) Scientific Research in Information Systems: A Beginner's Guide (2nd edition). Springer doi:10.1007/978-3-030-85436-2

Scholtz B. Govender J. & Gomez J. M. (2016). Technical and environmental factors affecting cloud computing adoption in the South African public sector. In CONF-IRM 2016 Proceedings (p. 16). http://aisel.aisnet.org/confirm2016/16

Seip Å. (2020). Sourcingstrategier for IKT i offentlig sektor. (FAFO Rapport 17/2020). Retrieved from: https://fafo.no/images/pub/2020/20752.pdf

Steen R. (2022). Skytjenester for offentlig sektor. (FAFO Rapport 22/2022). Retrieved from: https://www.fafo.no/images/pub/2022/20825.pdf

Svärd P. (2019) "The impact of new public management through outsourcing on the management of government information: The case of Sweden" Records Management Journal Vol. 29 No. 1/2 pp. 134-151. https://doi.org/10.1108/RMJ-09-2018-0038

Tafti M.H.A. (2005) Risks factors associated with offshore IT outsourcing Industrial Management & Data Systems Vol. 105 No. 5 pp. 549-560. https://doi.org/10.1108/02635570510599940

The Archives Act. (1992). The Archives Act (LOV-1992-12-04-126). Retrieved from: https://lovdata.no/dokument/NL/lov/1992-12-04-126/KAPITTEL_2#%C2%A79

The Norwegian Ministry of Local Government Strategy and Modernization (KMD). (2015). Cloud computing strategy for Norway. Retrieved from: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

The Norwegian National Security Authority (NSM). (2020). Helhetlig digitalt risikobilde 2020. Retrieved from: https://nsm.no/getfile.php/134267-1601027852/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2020_1609_LR.pdf

The Norwegian National Security Authority (NSM). (2023). Uforutsigbare tider krever høyere beredskap - Nasjonal sikkerhetsmyndighet. Retrieved from: https://nsm.no/aktuelt/risiko-2023-uforutsigbare-tider-krever-hoyere-beredskap

The University of Edinburgh. (2022 29. August). A general guide on how to conduct and write a literature review. Retrieved from:

https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review

Thomas D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. American Journal of Evaluation 27(2) 237–246. https://doi.org/10.1177/1098214005283748

Wold, G., Fylkesnes, T. K., Fiskaa, I., Øvstegård, F. A., Bergstø, K., & Hassel, S. B. (2022). Offentlige skytjenester for kommunal sektor. The Norwegian Parlament. (Proposition 48 S) Retrieved from: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2022-2023/dok8-202223-048s/?all=true

Wulf F. Strahringer S. & Westner M. (2019). Information security risks benefits and mitigation measures in cloud sourcing. In 2019 IEEE 21st Conference on Business Informatics (CBI) (pp. 258-267). IEEE. https://doi.org/10.1109/CBI.2019.00036

Xiao M. & Watson M. (2019). Guidance on Conducting a Systematic Literature Review. Sage Journal 39(1) 93-112. Retrieved from: https://doi.org/10.1177/0739456X17723971

Xiao Z. & Xiao Y. (2012). Security and Privacy in Cloud Computing. IEEE Communications Surveys & Tutorials 15(2) 843-859. doi:10.1109/SURV.2012.060912.00182

Yin R. K. (2017). Case study research and applications: Design and methods. Los Angeles CA: Sage.

Yin R.K. (2003). Case Study Research: Design and Methods. Sage. Thousand Oaks California.

APPENDIX A: CONSENT FORM

Vil du delta i forskningsprosjektet?

«Cyber sikkerhet ved adopsjon av skytjenester i offentlig sektor»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å *hvor formålet er å identifisere cybersikkerhets sårbarheter i offentlige organisasjoner ved adopsjon av skytjenester*. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Prosjektets formål er å identifisere hvordan adopsjonen av skytjenester har påvirket cybersikkerheten innenfor den offentlige etater. Mitt mål er å identifisere hvilke utfordringer bransjen står overfor som følge av skytjenesteleverandører, og hvilken påvirkning skytjenester har hatt på anskaffelsen av nye tjenester.

Dette er en masteroppgave innenfor Cybersikkerhet ved Universitetet i Agder, og resultatet vil være en forskningsrapport som tar for seg følgende spørsmål:

1. Hvorfor er cybersikkerhet i nåværende anskaffelser av skybaserte løsninger i offentlige etater utfordrende?
2. Hva er de cybersikkerhetsproblemene som offentlige etater opplever når de anskaffer seg skybaserte løsninger?
3. Hvordan kan offentlige etater sikre cybersikkerhet når de tilpasser seg skybaserte løsninger?

Rapportens forskningsperiode er definert fra 2. januar 2023 til 2. juni 2023 og informasjonen som presenteres i rapporten skal kun brukes til akademisk formål. Formålet er å gi best mulig svar på forskningsspørsmål og problemstillingen som er undersøkt.

Hvem er ansvarlig for forskningsprosjektet?

Prosjektet er underlagt Universitetet i Agder, ved Campus Kristiansand.

Hvorfor får du spørsmål om å delta?

Utvalget for undersøkelsen begrenses til fagpersoner som innehar relevant kompetanse og som aktivt sikrer svært høy integritet i den innsamlede informasjonen. Utvalgskriteriene inkluderer personell som besitter kunnskap innenfor områder som IKT, cybersikkerhet, leverandørkjede og/eller offentlig anskaffelse. Hensikten med å samle inn opptil 8 svar er å skape et solid faglig grunnlag og sikre svært høy integritet i den innsamlede informasjonen.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet ved å gjennomføre et intervju, vil det ta omtrent 45 minutter av din tid. Intervjuspørsmålene vil omhandle digitalisering, datasikkerhet og tredjepartsleverandører i offentlige etater, samt hvilken rolle du har i din organisasjon. Jeg vil gjennomføre intervjuet på nettet for å sikre effektivitet.

For å sikre nøyaktighet i den innsamlede informasjonen, vil intervjuet bli tatt opp på lyd. Disse opptakene vil bli slettet når prosjektet er ferdig. All informasjon som du deler vil bli registrert elektronisk og anonymisert for å beskytte ditt personvern.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

Personer som har ansvar for behandling av informasjonen, inkluderer veiledere ved Universitetet i Agder og prosjektgruppen. Tilgangskontrollen er begrenset til prosjektgruppen, som vil sørge for at uvedkommende ikke får tilgang til personopplysninger. Vi vil ikke bruke enkeltpersoners navn i prosjektet, da dette ikke er relevant for forskningen.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Vi vil anonymisere all informasjon når prosjektet er fullført og oppgaven er godkjent, som planlegges å være 2. juni 2023. All personlig informasjon vil bli slettet etter at prosjektet er avsluttet og oppgaven har blitt vurdert og karakterisert. Dette inkluderer fjerning av lydopptak, skjermopptak, intervju notater og annen sensitiv informasjon.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Agder, Kristiansand har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

Student ved Universitetet i Agder. Trygve Valbø. Mail:

trygvev@uia.no

Veileder ved Universitetet i Agder. Paolo Spagnoletti. Mail:

paolo.spagnoletti@uia.no

Vårt personvernombud: Trond Hauso. Mail:

personvernombud@uia.on

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen
Trygve Valbø
Student cybersikkerhet
Universitetet i Agder
Campus Kristiansand

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «cyber sikkerhet ved adapsjon av skytjenester i offentlig sektor», og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju-
- taleopptak av intervjuet (via UiO Nettskjema Diktafon)-
- at mine opplysninger behandles frem til prosjektet er avsluttet.

(Signert av prosjektdeltaker, dato)

APPENDIX B: INTERVIEW QUESTIONS

Intervjuguide

Hei, er i prosessen med å skrive masteroppgave i cybersikkerhet. Oppgaven våres er å prøve å finne “Hvorfor er cybersikkerhet i dagens anskaffelser av skyløsninger i norske kommuner utfordrende?” Hva er sikkerhetsproblemene som hindrer adopsjon og hvordan løser man det?

Først vil vi takke for at du stiller til intervju med oss i dag. Vi vil poengtere at det er helt frivillig å delta og at du ikke skal føle deg presset til å svare gjennom hele intervjuet. ingen kommentar er helt greit. Vi vil også anonymisere deg i oppgaven min. jeg lurer på om det er greit at vi tar lydopptak slik vi kan transkribere svarene dine? Dette vil naturligvis bli slettet når vi er ferdig å transkribere.

Først kan du fortelle litt om deg selv?

1. Hvilken rolle har du i din organisasjon?
2. Hvor lenge har du jobbet for organisasjonen?
3. Har du erfaring og eller utdanning fra IT-sikkerhet?

OM ORGANISASJONEN

1. hvilken typer IT trusler står dere ovenfor i dag?
2. Er dere avhengig av skyleverandører for å kunne levere tjenestene deres?
3. om ja hvordan?

En generell oversikt over kommunen som organisasjon.

1. Hvem er brukerne av systemene dere har?
2. Hvordan er organisasjonsstrukturen deres i dag?

Sikkerhetsutfordringer og -problemer

1. Hvilke sikkerhetsproblemer har kommunen opplevd ved å tilpasse seg skytjenester?
2. Er det noe som hindrer dere å benytte skyløsninger?

Tilgang og kontroll

4. Hvordan håndterer kommunen tilgangsstyring og konfidensialitet i skytjenester?
Hvor lagres data i dag lokasjon?

Hvor blir dataen deres lagret og prosessert geografisk? Hvordan vurderer dere risikoen for prosessering og lagring i utlandet?

Kunnskap og opplæring

6. Hva slags opplæring og støtte tilbys ansatte for å redusere menneskelige feil og øke kunnskap om skytjenester?

Ledelse og ansvar

1. Hvordan er ledelsens involvering og ansvar i håndtering av cybersikkerhet relatert til skytjenester?

2. Hvilke tiltak tar ledelsen for å sikre at organisasjonen har tilstrekkelig ressurser og kompetanse innen cybersikkerhet og skytjenester?
3. Hvordan bidrar ledelsen til å utvikle og implementere sikkerhetsstrategier og tiltak i forbindelse med bruk av skyløsninger?

Juridiske utfordringer

8. Hvordan navigerer dere gjennom komplekse lover og regler for datalagring, som GDPR, arkivloven og retningslinjer fra regjeringen, spesielt for lagring av data utenfor Norges grenser?

Tilgjengelighet

9. Hvilke tiltak har kommunen implementert for å sikre tilgjengelighet og kontinuitet i skytjenester? er det noen system som ikke er lagt på sky grunnet dette

Tillit og ressurser

10. Hvordan bygger kommunen tillit til skytjenesteleverandører, og hvordan påvirker dette valget av leverandører og tjenester?
11. opplever dere makt forskjell med leverandørene, der det er lite valg av leverandører?
12. Har dere tilstrekkelig med ressurser og kompetanse for å håndtere anskaffelser av skyløsninger? Er situasjonen lik når det gjelder generelle innkjøp?

Supply chain

1. Hvem er leverandørene deres til de største fagsystemene deres?

2. Hvordan forsikrer dere at leverandørkjeden til skytjenestene forsikrer at det har god sikkerhet.

3. Hvordan vet dere at underleverandører følger krav som dere pålegger dem

Serviceavtaler databehandleravtaler og sikkerhet

13 Hvordan sikrer dere kontroll over hele leverandørkjeden fra et sikkerhetspersståtsted?
14. Hvordan inngår og håndhever kommunen serviceavtaler (SLA) med skytjenesteleverandører for å sikre tjenestekvalitet og sikkerhet?

15. Hvilke sikkerhetsverktøy og -praksis benytter kommunen for å beskytte data og tjenester i skyen?

17Hvordan er ikt sikkerhet sikret gjennom kontrakter og avtaler nedover leverandørkjeden?

Valg av skytjenesteleverandører

1. Har dere opplevd at dere har blitt låst til en leverandør tidligere? Hva gjør dere for å unngå dette i fremtiden?

2. Hvordan tar kommunen hensyn til flerbrukermiljø (multitenancy)(Shared infrastructure) og mangel på kontroll over data og tjenester i skyen?

Strategi og retningslinjer

1. Hvordan jobber kommunen med å utvikle en strategi for skytjenester og sikkerhet som er i tråd med nasjonale og lokale myndigheters retningslinjer?

2. Hvordan forholder dere dere til offentlige retningslinjer for cybersikkerhet? Er det tilstrekkelig klare og forståelige?
3. Hvilke strategier og tiltak kan norske offentlige etater iverksette for å styrke cybersikkerheten i forbindelse med bruk av skyløsninger?

APPENDIX C: LITERATURE REVIEW PROTOCOL

This review protocol is defining the scope of the literature review and its initial aim is to get an answer on these research questions:

- **What are the cybersecurity challenges experienced by public organizations during the adoption of cloud solutions, and how can they address these concerns?**
    - **What are the security issues that public organizations experience when adopting cloud solutions?**
    - **How can public organizations ensure cyber security when adopting cloud solutions?**

From these research question I have defined inclusion and exclusion criteria for the literature review.

Table 4 Inclusion Criteria

Inclusion criteria	Reasoning
Must be related to the topic domain	The topic must consist at least about ICT outsourcing/offshoring.
The article should be related to cyber security	Since this thesis is a cyber security thesis, and the aim of the research question is strictly cybersecurity related the articles should be related to cyber security.
Must be formally published	The article must be published formally.
The article must be in either Norwegian or English	This criterion is set because to ensure that the articles are not in other languages that I do not understand.

Must contain keywords relating to our research question	This is to ensure that the topics is related to outsourcing or cloud computing. This is circuital to filter out irrelevant articles that are not relevant to the topic.

Table 5 Exclusion criteria

Exclusion Criteria	Reasoning
Not relevant to the topic domain	The topic that is not related to some form of ICT-outsourcing will be excluded.
Not published formally	Unpublished articles, or articles that are published on non-recognized journals will be excluded.
Article is not published in either Norwegian or English	Publication language that are not in either Norwegian or English will be excluded
The articles that are not finalized	Articles that is not complete will be excluded as the results cannot been seen as reliable.

These are the established criteria for evaluation. The title, abstract, and full text of each source will be assessed for relevance to the topic.

Table 6 Search strategy

Electronic databases

Google scholar	
Web of science	
Emerald	
Science Direct	
Keywords	Synonym/related concept (Abbreviation)
Security issues	Security problems
Outsourcing	Offshoring
IT-infrastructure	IT, Deployment
Government	Public
Cloud computing	Cloud, adaptation
Reference searches	
The project will be supplemented by conducting a backward searching for additional knowledge.	

APPENDIX D: LITERATURE LIST

Table 7 Literature List

Author	Main topic	Secondary topic
	Cloud solutions	Outsourcing
Nakatsu & Iacovou (2009)		X
Hamlen & Thuraisingham (2013)		X
Dhillon, Syed & Soarés (2017)		X
Khalfan (2004)		X
Bhatti, Mubarak & Nagalingam (2021)		X
Khidzir, Mohamed & Arshad (2010)		X
Pai & Basu (2007)		X
Hansen, Kraemmergaard & Mathiassen (2011)		X
Tafti (2005)		X
Bachlechner, Thalmann & Maier (2004)		X
Nassimbeni, Sartor & Dus (2011)		X
Xiao & Xiao (2013)	X	
Almutairi & Riddle (2018)		X
Svärd (2018)		X
KMD (2015)	X	
Svantesson (2011)	X	
Kyeiakou, Euripides & Paraskevi (2020)	X	
Steen (2022)	X	
Seip (2020)	X	

NSM (2020)	X	X
Ghaffar (2020)	X	
Wulf, Strahringer & Westner (2019)	X	
Kishetri (2013)	X	
Pearson & Benameur (2010)	X	
Abdullah & Quintero (2019)	X	
Scholtz, Govender & Gomez (2016)	X	
Ali & Osmanaj (2020)	X	
Kajiyama, Jennex & Addo (2017)	X	
Polyviou & Pouloudi (2015)	X	