Understanding the Phenomenon of Cloud Computing Adoption within Organizations

Rania El-Gazzar

Understanding the Phenomenon of Cloud Computing Adoption within Organizations

Doctoral Dissertation 129

University of Agder
Faculty of Social Sciences
2016

Doctoral Dissertations at the University of Agder 129

ISSN: 1504-9272
ISBN: 978-82-7117-822-2

Printed by the Printing Office, University of Agder
Kristiansand

This thesis has been submitted at the

Department of Information Systems

Faculty of Social Sciences

University of Agder, Kristiansand, Norway

In partial fulfillment of the requirements for the

Ph.D. degree in Information Systems

Defense Date: June 1st 2016

Opponents

Tero Päivärinta, Professor

Luleå University of Technology, Sweden

Karin Bernsmed, Adjunct Associate Professor[1], Research Scientist[2]

[1]Norwegian University of Science and Technology (NTNU), [2]SINTEF ICT, Norway

Maung Kyaw Sein, Professor

University of Agder, Norway

Supervisors

Eli Hustad, Associate Professor

University of Agder, Norway

Dag Håkon Olsen, Professor

University of Agder, Norway

Acknowledgement

I would like to begin by expressing my sincere appreciation to everyone who supported me; without them I would not have had the spirit to complete this work. I would like to thank the Faculty of Social Sciences at University of Agder for their spiritual, financial and official support; in particular, I would like to thank Inger-Lise Myrvold, Målfrid Tangedal, and Harald Stokkeland. I would also like to extend my sincere gratitude to the Department of Information Systems for giving me the academic, educational, and inspirational support to survive my PhD journey. I am indebted to Bjørn Erik Munkvold, the Director of our PhD programme, for never failing to follow up on our PhD progress, and for listening to our needs and struggles.

To my supervisors, Eli Hustad and Dag Håkon Olsen, I am extremely grateful for your guidance, co-authorship, and suggestions throughout my PhD journey. I extend my gratitude to Carl Erik Moe, Jon Iden, and Tom Roar Eikebrokk for their rapid response to any queries I raised during the Delphi study. I further extend my gratitude to Peter Axel Nielsen for his constructive feedback on an early draft of my second publication.

I am extremely grateful to Helle Zinner Henriksen for her critical and constructive feedback on an early draft of this thesis, which strengthened its content and left it in better shape.

To all my friends, thank you for helping me survive the stresses of the past three years and for not letting me give up. I especially thank Karen Stendal, Soffi Westin, Adeola Wale-Kolade, Torbjørg Meum, Bente Elisabeth Holmen, Alfatika Aunuriella Dini, Moutaz Haddara, Fathul Wahid, Christoph Merschbrock, Øyvind Hellang, Niels Frederik Garmann-Johnsen, Luay Anaya, Geir Inge Hausvik, and Peter Busch for the fun times and the insightful discussions and advices we had about research and all matters life-related. To Fathul Wahid, Thank you for the co-authorship and inspiration.

A special debt of gratitude must go to my informants from academia and practice, both from the provider side and the client side, who agreed to be part of this work and shared their experiences on the topic I was investigating. I thank them for their insightful input and feedback, both of which enriched my study.

I thank Susan Watts for editing and polishing the thesis. Her efforts have made it read so well.

I owe a great deal of gratitude to my amazing Father Fahim El-Gazzar and my two lovely sisters Marwa and Rasha for supporting me with their warm love, deep understanding, wisdom, patience, encouragement, and for pushing me further than I thought I could go. My endless debt of gratitude goes to my beloved Mother Zahira Allam, whom I lost in the first year of my PhD. Her encouraging spirit accompanied me all the way, whispering to me to *"keep faith..."*.

List of Abbreviations

CC	Cloud Computing
IS	Information Systems
SaaS	Software-as-a-Service
PaaS	Platform-as-a-Service
IaaS	Infrastructure-as-a-Service
IT	Information Technology
EDS	Electronic Data Systems
SLA	Service Level Agreement
ASP	Application Service Provision/ Application Service Provider
SME	Small and Medium Enterprise
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
SOA	Service-Oriented Architecture
CEO	Chief Executive Officer
NIST	National Institute of Standards and Technology
CSP	Cloud Service Provider
VM	Virtual Machine
CSA	Cloud Security Alliance
SOA	Service-Oriented Architecture
CIO	Chief Information Officer
VPN	Virtual Private Network
HRM	Human Resources Management
ASPIC	Application Service Provider Industry Consortium

Abstract

The aim of this PhD thesis is to understand the phenomenon of Cloud Computing (CC) adoption through the following main Research Question (RQ):

How can we understand the phenomenon of CC adoption within organizations?

This research question is addressed by exploring two Sub Questions (SQs) which, through different accounts, explain the importance of the institutional factors' influence on CC adoption. These SQs are:

What are the institutional factors that affect CC adoption in organizations?

How do institutional factors shape CC adoption strategies?

The research study in this thesis has provided results based on three research methods: (1) a systematic literature review; (2) two case studies, one from Egypt, and a second from Norway, and (3) a ranking-type Delphi study in which three different subpanels of experts were involved who represented various stakeholders (i.e., clients, providers, and academics). This research took place from September 2012 until March 2015.

The total number of informants was 46 who have contributed to the empirical studies in terms of interviews and/or Delphi surveys. The aim of the research approach used was to provide rich insights into understanding the CC adoption phenomenon through the shared experiences of the informants involved and their different views on the same phenomenon. In particular, I aimed to gather additional data related to the Egyptian and Norwegian contexts. By including the different views of informants from different contexts and domain backgrounds on the same phenomenon, this thesis was able to identify a breadth of institutional factors and CC adoption strategies.

Part of the data analysis was carried out by applying statistical methods to generate results from the narrowing-down and ranking surveys of the Delphi study. Furthermore, the inputs from the brainstorming questionnaire were coded to generate the consolidated list of CC adoption issues. The other part of the analysis was carried out using concepts from neo-institutional theory; these concepts are isomorphic pressures and strategic responses to institutional processes. The results generated from applying neo-institutional theory and statistical methods were triangulated to identify: (1) the external and internal institutional factors that influence, either by facilitating or hindering the adoption of CC services in organizations, and (2) CC adoption strategies.

The findings from this thesis indicate that the CC adoption phenomenon can be understood through the external and internal institutional factors that have an important influence on CC adoption strategies. These adoption strategies are shaped by the interplay of institutional factors. Hence, in this thesis, eight institutional factors have been identified, together with three CC adoption strategies that are shaped by these factors. Five external factors have been identified that are related to the external social environment, both locally and globally (i.e., governments and regulatory bodies, cloud providers, media, socio-political changes, and culture). Three internal factors have been identified that are related to the internal social and technical environment of organizations (i.e., internal stakeholders, firm characteristics, and IT infrastructure). The importance of these factors identified from the Delphi rankings indicates that organizations are encouraged take them into consideration when adopting CC services. The identified strategies are: efficiency-motivated adoption, legitimacy-motivated adoption, and non-adoption. Furthermore, the findings from this study are compared with the research gaps that exist in the literature.

This thesis offers contributions to: (1) the area of CC adoption by identifying external and internal institutional factors and CC adoption strategies through a mixed research approach of quantitative and qualitative methods. This has created a rich understanding of CC adoption phenomenon and (2) utilizing the neo-institutional theory to achieve a broader and richer understanding of the CC adoption phenomenon.

In addition, this thesis offers implications for practice. From the brainstorming phase of the Delphi study, a list of 55 identified issues has been generated to be of concern regarding the adoption of CC. These issues have been coded and grouped into 10 categories: (1) security, (2) availability, (3) migration, (4) business, (5) legal and ethical concerns, (6) culture, (7) awareness, (8) impact, (9) strategy, and (10) IT governance. These issues are suggested by the Delphi panelists as important for executives and managers in general to take into account when considering CC investments.

The practical implications of this study are aimed at clients, cloud providers, and law-makers. Clients need to: (1) have a business case that is driven by business needs rather than IT costs, and (2) make a good estimation of the required change and communicate this with internal stakeholders in a convincing way. Cloud providers need to: (1) be strategic in sensing the different demands of different markets, and reflecting these demands in their marketing campaigns, and (2) consider clients'

security requirements, which differ from the security already on offer. Law-makers need to learn from the financial industry about how to build an ecosystem for the global exchange of data rather than money in the cloud; such an exchange must be based on trust and international governance practices.

This thesis also offers several opportunities for future research. In particular, it points to the benefits of a comparative analysis (e.g., countries and/or sectors) using a new theoretical lens such as management fashion. This would provide an insight into how cloud providers, consultants, governments, and academics perceive different market demands, and how they respond to these demands when promoting CC services.

This thesis also encourages IS researchers to: (1) explore factors that influence the adoption of particular service models (e.g., SaaS, PaaS, and IaaS or public, private, and hybrid), and (2) conduct longitudinal studies on CC adoption, which can provide valuable implications on the entire CC adoption experience.

Last but not least, the results from the Delphi study indicate the need for further research on the various concerning CC adoption issues that were revealed among the panelists.

The contributions of this thesis are based on incorporating the empirical work published in five papers.

Table of Content

1 Introduction 17

1.1 Research Questions 19

1.2 Structure of the Thesis 20

2 Background and Related Research 25

2.1 An Evolutionary History of IS/IT Outsourcing Adoption Leading to Cloud Computing Services 25

2.2 IS/IT Outsourcing Adoption Research 30

2.3 Cloud Computing As An Emerging IS/IT Outsourcing Model 34

2.4 A Systematic Literature Review on Cloud Computing Adoption Research 41

2.5 Summary of the Chapter 47

3 Theoretical Foundation 51

3.1. Neo-Institutional Theory 51

3.2. Neo-institutional Theory in IS Research 54

3.3. Neo-institutional Theory and Cloud Computing Adoption 57

3.4. Summary of the Chapter 61

4 Research Approach 65

4.1. Research Design 65

4.2. Research Activities 68

4.3. Getting Informants Onboard 70

4.4. Data Collection and Analysis 76

4.4.1. Ranking-type Delphi Study 77

4.4.2. Selection of Cases 84

4.4.3. Interviews 96

4.4.4. Secondary Data Sources 98

4.4.5. Data Analysis 100

4.5. Validity Issues 111

5 Research Publications 121

5.1. Paper1: Defining External Pressures and CC Strategies 122

5.2. Paper2: A Literature Review 123

5.3. Paper3: Egypt Case Study 124

5.4. Paper4: Norway Case Study 125

5.5. Paper5: Delphi Study 126

5.6. Bringing Together the Whole Story 128

6 Discussion of Main Findings 133
6.1. Understanding The Adoption of CC Services 133
6.2. Institutional Factors in the Context of CC Adoption 135
6.2.1. External Factors 135
6.2.2. Internal Factors 144
6.3. Institutional Factors and CC Adoption Strategies 149
7 Contributions 155
7.1. Contributions to Knowledge and Theoretical Implications 155
7.1.1. CC Adoption 157
7.1.2. Neo-institutional theory 162
7.2. Implications for Practice 173
8 Conclusion, Limitations, and Future Work 179
8.1. Summary 179
8.2. Limitations and Generalization Issues 180
8.3. Future Research 182
9 Reflections 185
References 191
Appendix A: Research Publications 207
Appendix B: Documentation of Data Collection and Data Analysis 315

List of Figures

Figure 1: Cloud computing adoption rates in 2013 and 2014 18
Figure 2: History of IS/IT outsourcing 27
Figure 3: Cloud computing adoption factors and processes (Paper2) 44
Figure 4: Research design 68
Figure 5: Overview of research activities 69
Figure 6: Overview of the Delphi study process 79
Figure 7: Example (1) of analyzing the Delphi's list of 55 issues based on the feedback round 101
Figure 8: Example (2) of analyzing the Delphi's list of 55 issues based on the feedback round 102
Figure 9: Data analysis procedures followed 106
Figure 10: Analysis example 1 108
Figure 11: Analysis example 2 109
Figure 12: Analysis example 3 110
Figure 13: The analytical framework for understanding cloud computing adoption 123
Figure 14: Relationships between publications 129
Figure 15: Understanding cloud computing adoption phenomenon 135
Figure 16: Contributions in light of the neo-institutional theory 166

List of Tables

Table 1: Scenarios for deploying CC services (adapted from CSA, 2009) 35
Table 2: Isomorphic pressures (DiMaggio & Powell 1983) 53
Table 3: Strategic responses to institutional processes (Oliver 1991) 53
Table 4: Organizations at the field level (Paper1) 59
Table 5: Isomorphic pressures (Paper1) 60
Table 6: Strategic responses (Paper1) 60
Table 7: Informants' profile 73
Table 8: Delphi study design 78
Table 9: Summary of reasons for the selected case studies 95
Table 10: Interviews's profile 98
Table 11: Secondary data sources 99
Table 12: Sample codes of interview quotes 104
Table 13: Distribution of panelists by stakeholders group and by country 112
Table 14: Validity issues of the Delphi study 115
Table 15: A summary of the validity issues according to principles for IS interpretive research 116
Table 16: List of publications 121
Table 17: Relationships between publications and research questions 122
Table 18: Summary of the contributions 156
Table 19: Summary of implications for practice 173

“The framing of a problem is often far more essential than its solution.”

— Albert Einstein

1 Introduction

This thesis focuses on understanding the external and internal factors that influence (either by enabling or inhibiting) the adoption of CC services in organizations.

Before exploring problem formulation, it is necessary to clarify the term *adoption,* because it will be frequently used throughout this thesis. In IS literature, the term is used either to refer to a single process, which is *decision* (Rogers 1995; Swanson & Ramiller 2004), or to a sequence of several stages such as initiation, adoption, implementation (Thong 1999). Furthermore, the term is used interchangeably with several synonyms such as *decision*, *use*, *diffusion*, and *acquisition* (Schneider & Sunyaev 2014). In this thesis, the term *adoption* is related to the CC adoption processes as they appear in the literature; this includes the decision as to whether or not to adopt CC services. The focus is also on the factors that influenced the "adoption" or "non-adoption" decision, and, after the "adoption" decision. The term "adoption" also includes proof of concept as well as implementation and use. According to Rogers (2003), non-adoption refers to the rejection of an opportunity to adopt an innovation. Such a rejection can be classified as either: active (where the innovation was adopted earlier, but later on, a non-adoption decision is made) or passive (where no thought is given to the adoption of an innovation at all). In this thesis, non-adoption refers to the fact that, even though consideration was given to the adoption of CC services, adoption is eventually rejected because of external or internal factors.

We are witnessing a growing interest in CC that *"entails firms selling computing rather than computers to clients. Servitization strategies allow an organization to shift from selling a product to selling an integrated product and service offering"* (Barrett et al. 2015, p.137). On the other hand, there is a growing concern from clients about this new business model; thus, there is need to gain more knowledge about its dynamics.

The technological development of CC services is growing faster than its adoption rates (Linthicum 2013). A comparison of survey results from two consecutive years, 2013 and 2014, indicates slow adoption rates (RightScale 2013; RightScale 2014). As shown in Figure 1, adoption rates in general are not even higher than 40%. Furthermore, non-adoption and adoption rates have only changed slightly (either increasing or decreasing) from 2013 to 2014. This implies that, whilst organizations

have sought to leverage the benefits of using CC services, they are still facing challenges that slow down their adoption.

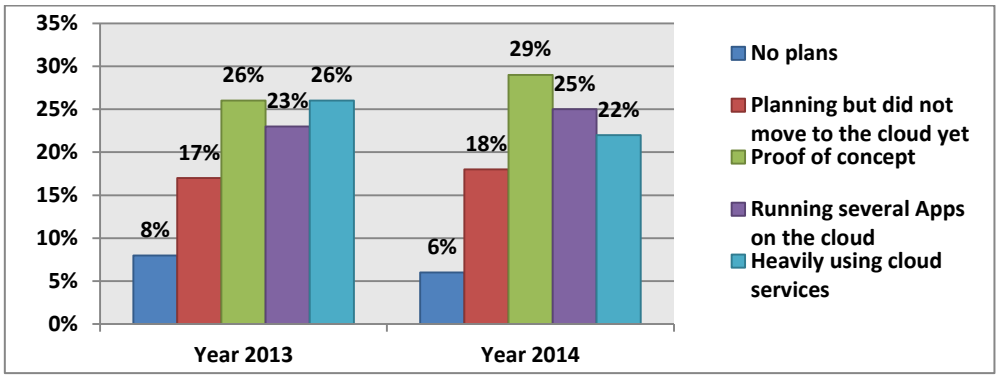


Figure 1: Cloud computing adoption rates in 2013 and 2014

Adoption rates are adapted from sources (RightScale 2013; RightScale 2014) **and combined into one graph**

Despite the capabilities that the CC model can bring to organizations in terms of scalability, flexibility, agility, simplicity, and efficiency (Venters & Whitley 2012), there are nonetheless several critical factors to its adoption. These factors are related to technology, business environment, the potential adopting organization, and the relationship between the potential adopting organization and its business environment (Armbrust et al. 2010; Garrison et al. 2012; Marston et al. 2011). The existing IS literature has indicated the lack of research in the area of CC adoption and the need for practice-related IS research outcomes (Yang & Tate 2012). Furthermore, there is a need to transfer lessons learned from cross-country investigations, which may reveal more influential factors in the adoption of CC services (Schneider & Sunyaev 2014). Furthermore, recent literature has advocated the need for studying the "adoption" and "non-adoption" of CC services, because it would be interesting to compare non-adoption with adoption (Schneider & Sunyaev 2014).

This thesis is motivated by the above statements and by a desire to take a rather broad perspective that includes the adoption of various CC service models (i.e., SaaS, PaaS, and IaaS), deployment models (i.e., public, private, and hybrid), organization types (i.e., public and private), and contexts (i.e., developed versus developing countries). Hence, the scope of this thesis is to understand CC adoption as a phenomenon that is influenced by a set of internal and external factors. The empirical setting for achieving this research aim necessitated the use of three research methods: (1) a systematic literature review to identify factors that have been found to influence the adoption of CC services in existing research; (2) two case studies, one about a developing country (Egypt), and a second about a developed country (Norway). Institutional factors are identified based on an analysis of both contexts; and (3) a Delphi study that was conducted by setting up three subpanels to represent the various stakeholders (i.e., clients, providers, and academics).

This research resulted in contributions to both literature and practice. The contribution of this thesis was its revelation of a breadth of external and internal factors that are perceived to be most important to the adoption of CC services and yet are not well highlighted in the literature. The implications for practice can assist decision-makers in adopting CC services properly.

1.1 Research Questions

The main research question (RQ) of the thesis is:

> *RQ: How can we understand the phenomenon of CC adoption within organizations?*

Two sub questions (SQ) were formulated to answer the main RQ. To answer the research questions, I chose the interpretive research approach to understanding the CC adoption phenomenon (Walsham 2006), together with the case study method, because it is an appropriate method for addressing *how* questions (Yin 2009). I first started my research inquiry by carrying out the Delphi study to explore and rank the most important topics (or issues) in the area of CC adoption. The Delphi study then guided my choice of the two case studies, one from Egypt and one from Norway. Using the case study method along with the lens of neo-institutional theory, I aimed to understand the CC adoption phenomenon by exploring the external and internal institutional factors related to the Egyptian and Norwegian contexts that affect the adoption of CC services. These two contexts are different both in terms of socio-economic and socio-political status. The literature has reported the limited research findings on the institutional factors that influence CC adoption (Schneider & Sunyaev 2014). Neo-institutional theory is a suitable lens for understanding how external and internal factors influence the adoption of IS/IT innovations in organizations that exist in different socio-economic and political contexts (Weerakkody et al. 2009). Furthermore, the follow-up interviews that I conducted with the informants who participated in the Delphi study revealed further internal and external factors. These research methods constituted my response to the first SQ:

> *SQ1: What are the institutional factors that affect CC adoption in organizations?*

I further aimed to identify the importance of these factors; indeed, both the case studies and the Delphi study provided evidence on this. The case studies showed the importance of these factors through their influence on the strategies used for adoption , while the Delphi study provided rankings. Thus, my response to the second SQ can be formulated as:

SQ2: How do institutional factors shape CC adoption strategies?

I have positioned my research to be interpretive despite using the term "factors", which may indicate positivism. Furthermore, I have built my understanding of the institutional factors and how they shape CC adoption strategies based on the field data. Thus, both the factors and their influence, as well as the CC adoption strategies used, emerged from my informants' interpretations and shared meanings, rather than from hypothetic-deductive logic and analysis (Orlikowski & Baroudi 1991).

1.2 Structure of the Thesis

In this thesis, I present the contributions made by my five research papers (Appendix A). Each paper is considered a *part* of my overall research. I will also refer to some of the content of these papers in subsequent chapters of this thesis in order to offer further insight into my argument as a *whole*.

This thesis is divided into eight chapters. In Chapter 1, I present the problems raised by the thesis, together with its aim, and scope.

Chapter 2 provides a background on IS/IT outsourcing and CC and explores the contributions made by selective IS studies to IS/IT outsourcing adoption. An introduction to the systematic literature review conducted on CC adoption in Paper2 is then given. Thereafter, I offer a summary of the chapter.

In Chapter 3, I provide the background to neo-institutional theory and its concepts, before going on to offer an argument for my theoretical choice. I review selective IS literature in terms of how the theory has been applied in the areas of IS and IS/IT outsourcing. Then, I review the limited IS research stream that has applied neo-institutional theory to study CC phenomenon. Thereafter, I introduce my first publication, in which I have defined the organizational field, isomorphic pressures, and strategic responses in the context of CC based on literature. I finish by offering a summary of this chapter.

Chapter 4 provides details of the research approach taken in this thesis, including research design, activities, data collection, and data analysis. I end the chapter by reflecting on the validity issues related to my research approach.

Chapter 5 summarizes the contribution of each individual publication to this thesis as a whole. The link between the publications and the research questions is demonstrated (See Table 13 in Chapter 5). The chapter ends by presenting the overall research story of the thesis.

Chapter 6 presents a discussion of my findings and provides answer to the main RQ and the two SQs. In addition, I knit the contributions of the publications to appear as one consistent piece.

Chapter 7 presents the theoretical contributions made by this thesis in terms of its response to the main RQ and two SQs. Also highlighted is the contribution made to practice.

Chapter 8 concludes with a summary of the thesis, highlights limitations, and offers opportunities for the future work.

Chapter 9 provides my own reflections on this doctoral study.

The five research papers that generate the contribution of this thesis are:

1. Paper1: El-Gazzar, R., & Wahid, F. (2013). An Analytical Framework to Understand the Adoption of Cloud Computing: An Institutional Theory Perspective. In *Proceedings of the International Conference on Cloud Security Management (ICCSM2013)* (pp. 91–98). Academic Conferences and Publishing International.
2. Paper2: El-Gazzar, R. F. (2014). A Literature Review on Cloud Computing Adoption Issues in Enterprises. In *IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014* (pp. 214–242). Springer Berlin Heidelberg.
3. Paper3: El-Gazzar, R. F. (2015). The Start of a Journey to The Cloud in The Developing World : A Case Study of Egypt. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS 2015)* (pp. 4345–4354).
4. Paper4: El-Gazzar, R. F., & Wahid, F. (2015). Strategies for Cloud Computing: Insights from the Norwegian Public Sector. In *Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2015)*.
5. Paper5: El-Gazzar, R. F., Hustad, E., & Olsen, D. H. (2016). Understanding Cloud Computing Adoption Issues: A Delphi Study Approach. (Accepted for publication in the Journal of Systems and Software). The article is currently in-press: http://www.sciencedirect.com/science/article/pii/S016412121630036X.

“If the word doesn't exist, invent it; but first be sure it doesn't exist.”
— Charles Baudelaire

2 Background and Related Research

In Section 2.1, I offer an overview of the history of IS/IT outsourcing that led to the provision of CC services. In particular, I refer to the IS literature to trace the time frames during which various IS/IT outsourcing models emerged and evolved. In Section 2.2, I discuss IS literature on the adoption of IS/IT outsourcing. Thereafter, in Section 2.3, I provide a background on the CC model (i.e., definition, characteristics, and service models). In Section 2.4, I go on to discuss a systematic review I carried out on IS literature related to CC adoption (cf. Paper2). Finally, in Section 2.5, I offer a summary of the chapter.

2.1 An Evolutionary History of IS/IT Outsourcing Adoption Leading to Cloud Computing Services

"Nothing comes from nothing" - Parmenides

In this Section, I stand on the shoulders of the giant IS literature that has thoroughly investigated the IS/IT outsourcing adoption phenomenon. In particular, I review the history of the IS/IT outsourcing phenomenon, which evolved over time (See Figure 3), and examine existing definitions of IS/IT outsourcing models (Leimeister 2010). IS/IT outsourcing has been defined by Loh and Venkatraman (1992a) as the significant contribution made by external vendors to the physical and/or human resources associated with the entire or specific components of the IT infrastructure in the user organization. Lacity and Hirschheim (1993) defined it as the provision of or purchase of a product or service that could be provided within the buyer firm. According to Willcocks and Lacity (1997), IS/IT outsourcing can be defined as the delegation of the third party management of organizational assets, resources and/or activities to achieve a desired result. Kern and Willcocks (2000) defined it as a decision taken by an organization to outsource or sell an organization's IT assets, people and/or activities to a third party supplier, who in exchange provides and manages assets and services for monetary returns over an agreed time period. The latter definition encapsulates the three former definitions and adds more details to the meaning of IS/IT outsourcing. In the 1960s and 1970s, IS/IT outsourcing started off by being *technology-centric.* By the 1980s and 1990s, however, it had become more *business-centric*. Ever since then, it has become increasingly *industry-centric* (Currie & Seltsikas 2001; Cusumano 2010).

The term IS/IT outsourcing emerged in the 1960s along with the vision of *computing as a utility,* which started with the idea of *time sharing*, or the *service bureau.* At that time, IBM and the other major IT companies developed huge mainframes that most

businesses could not afford to build for themselves; thus, client organizations could access these mainframes using computer terminals (Lee et al. 2003). The role of third party suppliers came under the heading of *facilities management,* "where the vendor assumed operational control over the customer's technology assets, typically a data center" (Hirschheim et al. 2007, p.5). However, in 1963, an outsourcing contract was created between Blue Cross of Pennsylvania and EDS, which extended the supplier's responsibility to data centers and IS personnel (Dibbern et al. 2004).

From those early developments, IS/IT outsourcing adoption witnessed a tremendous growth, with major outsourcing contract arrangements being recorded in detail in the IS literature (Dibbern et al. 2004; Loh & Venkatraman 1992b). At that time, mainframes were having standard software packages already installed, such as operating systems and utility programs (Lee et al. 2003). These standard software packages did not meet the specific need of client organizations and customized software was expensive to develop in-house (Amant 2009). Thus, in the 1970s, the scope of IS/IT outsourcing extended to include outsourced software development, with the notion of *contract of programming* (Loh 2005; Amant 2009). This type of IS/IT outsourcing is considered as a one-to-one arrangement, where the service provider serves the unique needs of each client (Tebboune 2003).

In the 1980s, with the rise of *low-cost minicomputers and PCs*, many client organizations could financially afford to *maintain in-house computing capabilities*; thus, they decided to bring their outsourced services back in-house to gain more control over their IT assets (Amant 2009; Lee et al. 2003). In the IS literature, this was interpreted as *backsourcing* (Hirschheim et al. 2007). Thus, during the 1980s, the economically driven IS/IT outsourcing syndrome vanished. In 1989, it was revived once again when Eastman Kodak signed a 10-year large-scale contract with IBM ($500 million) to outsource four data centers and 300 IT personnel to IBM (Loh & Venkatraman 1992b). Known as the *Kodak effect,* it caused other organizations to once again jump on the bandwagon of IS/IT outsourcing, this time with a strategic focus to maintaining business success (Loh & Venkatraman 1992b; Lacity & Hirschheim 1993; Dibbern et al. 2004). Thus, the motivation for the revival of IS/IT outsourcing at this time was the desire to become a leaner organization and to avoid the hassle of upgrading applications internally (Amant 2009).

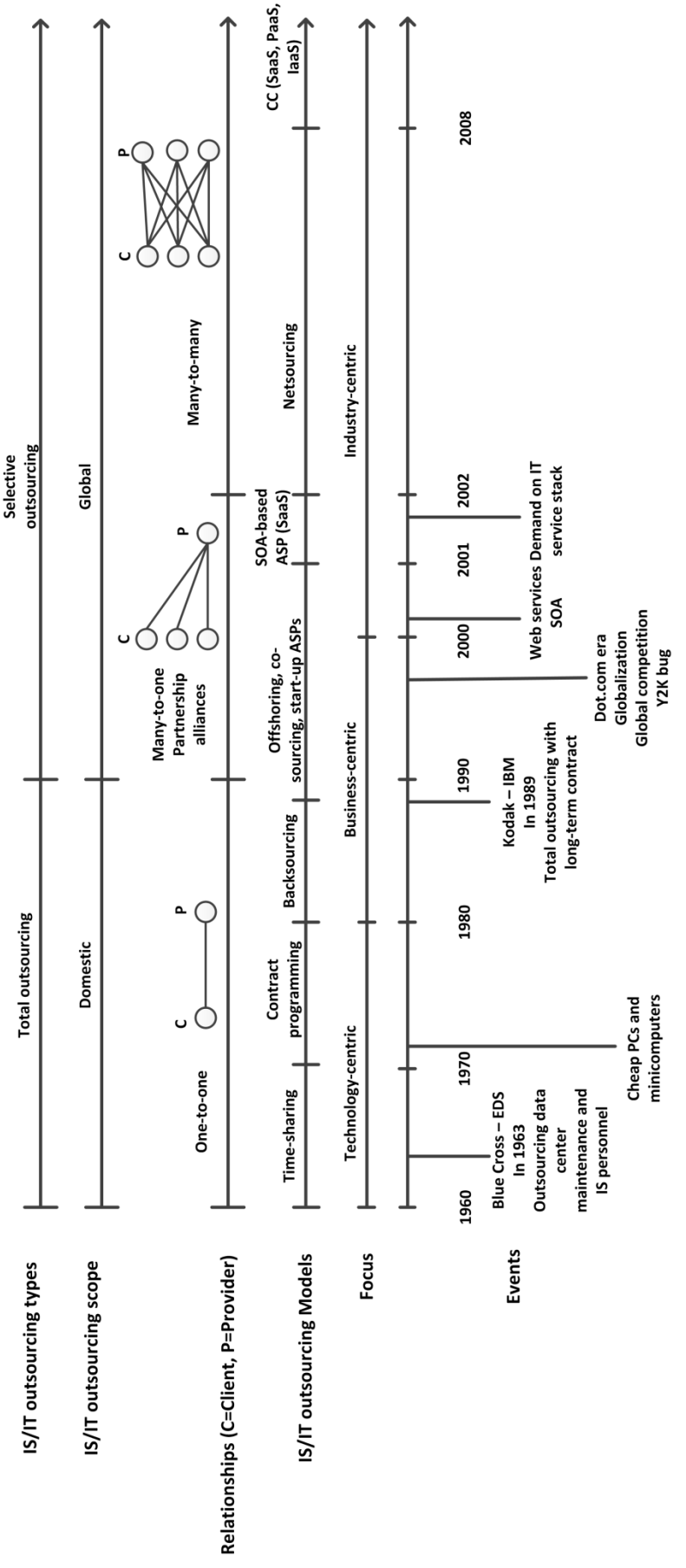


Figure 2: History of IS/IT outsourcing

The type of IS/IT outsourcing adopted by Kodak is known as *total outsourcing* in which "the vendor is in total charge of a significant piece of IS work" (Lacity & Hirschheim 1993, p.2), In some cases, this proved to be a poor strategy, leading to an increase in IT costs, because of poorly defined contracts (Lacity et al. 1996). Until the late 1980s, IS/IT outsourcing adoption patterns were *domestic*, *sole-sourcing (i.e., a one-to-one relationship),* and *total outsourcing*, "where one vendor provides all IT services to its client" (Hirschheim et al. 2007, p.5). However, in the 1990s, more complex IS/IT outsourcing arrangements emerged, including *one-to-many*, where one client organization signs an outsourcing contract with many IT vendors, and *many-to-many*, where many client organizations and many IT vendors sign one outsourcing contract (Gallivan & Oh 1999). In the 1990s, three adoption patterns of IS/IT outsourcing were prevalent. First, *selective outsourcing*, which was defined by Lacity et al. (1996) as a short-term contract of less than five years for a specific activity; it was argued to be the best practice at these times, because it could meet the needs of client organizations at minimum risk, in contrast with total outsourcing (Lacity & Willcocks 1998). Selective outsourcing emerged as an early form of offshore outsourcing (Amant 2009). Second, *offshore outsourcing* emerged as a result of the *globalization* and *global competition*, particularly during the dot.com era and as a result of concerns about the Y2K bug (Hirschheim et al. 2007; Amant 2009). In offshore outsourcing, the responsibility for managing and delivering IT services is transferred to a vendor located in a different country to that of the client organization, such as India, where labor is available at a low cost (Hirschheim et al. 2007; Sabherwal 1999). Third, c*o-sourcing* involves the establishment of a *partnership*, or *alliance* between the client organization and the vendor. It is based on the mutual exchange of benefits and risks (Lee et al. 2003; Hirschheim et al. 2007). Co-sourcing is known to be a *many-to-one alliance*, where many client organizations contract IT services from one vendor (Gallivan & Oh 1999).

Significant technological advancements (e.g., Internet speed and security, VPNs) have meant that another form of IS/IT outsourcing became attractive in the late 1990s, known as *application service provision* or *ASP* (Schwarz et al. 2009; Susarla et al. 2003). ASPIC[1] (now known as CompTIA) has defined an ASP provider as an entity that, *"manages and delivers application capabilities to multiple entities from a data*

[1] The Application Service Provider Industry Consortium (ASP Industry Consortium) is the global advocacy group promoting the application service provider industry by sponsoring research and articulating the strategic and measurable benefits of this delivery model. The ASP Industry Consortium was formed in May 1999. In 2001, the ASPIC merged into CompTIA and continues its mission within that organization.
(source: http://www.internetnews.com/asp-news/article.php/930561/ASP+Trade+Group+Joins+CompTIA.htm)

center across a wide area network (WAN)" (Susarla et al. 2003). ASP emerged as a first wave of Internet-based applications (Koutsoukis & Mitra 2003), where applications are hosted on and managed by an ASP provider's data center. The applications are made accessible remotely for client organizations through the Internet or VPN on a subscription basis (Schwarz et al. 2009). ASP represented a shift in IS/IT sourcing arrangements from owning, buying, and selling, to renting IT resources that are delivered over the Internet (Kern, Willcocks, et al. 2002). ASP is particularly attractive for businesses because of the low costs involved, the fast time to market, and easy access to IT expertise (Susarla et al. 2003; Lee et al. 2003). ASP is considered as an innovation and has gained a significant popularity from SMEs upon its rise as they are literally lacking in-house financial and technical competencies (Currie 2004).

ASP market witnessed two waves (Currie & Parikh 2006; Seltsikas & Currie 2002; Desai et al. 2003). The first wave was made up of *start-up ASP* providers, which used traditional IT infrastructure, but delivered application services through the Internet. However, start-up ASPs lacked the financial resources to upgrade the infrastructure to keep pace with new technologies such as web services, and, by 2001, it was no longer in the market. As per ASPIC's definition and according to Kern et al. (2002), this first wave of ASP resembled a *many-to-one* outsourcing arrangement. The second wave was made up of *web services providers*, who delivered applications known as *SaaS* through a web services-based SOA. Thus, they were able to offer agility and flexibility for client organizations to adapt to ever changing market demands. This second wave of ASP providers offered a variety of application services specific to industry (e.g., healthcare), business functions (e.g., marketing), enterprise processes (e.g., ERP), and pure-play (e.g., e-mail) (Schwarz et al. 2009). ASP allowed client organizations to access IT resources and expertise (e.g., license upgrading) that they could not afford to own themselves; hence, it offered client organizations business, technical, and economic benefits, as well as risks (Kern, Kreijger, et al. 2002).

Client organizations soon shifted from just needing to access stand-alone independent software vendors' software to a stack of IT services ranging from customization, training and delivery to integration. Thus, ASP providers started to rely on a variety of value-chain providers (Kern, Willcocks, et al. 2002; Kern, Kreijger, et al. 2002). Hence, the term *netsourcing* emerged in 2002, resembling a many-to-many outsourcing arrangement in terms of the various risks entailed. These included the subcontracting of a set of underpinning IT services by one supplier to another; however, such risks can be mitigated (Kern, Willcocks, et al. 2002). Netsourcing

appeared in a well-cited book, "Netsourcing: Renting Business Applications and Services Over a Network", by Kern et al. (2002), who defined netsourcing as *"the practice of renting or "paying as you use" access to centrally managed business applications, made available to multiple users from a shared facility over the Internet or other networks via browser-enabled devices"*. The authors viewed netsourcing as a *service stack* model from a layered infrastructure perspective (i.e., network services, hosting, application operations, and application access, respectively). Netsourcing implies that client organizations may adopt any, or all, of the stack (Kern, Lacity, et al. 2002).

In 2008, the term *cloud computing* (CC) came into being, with claims that it is a dream come true for those who believe in the notion of "computing as a utility" (M. Armbrust et al., 2009). There was some debate among executives as to whether CC is a different model of IS/IT outsourcing or a different term altogether (Armbrust et al. 2009, p.3):
"The interesting thing about Cloud Computing is that we've redefined Cloud Computing to include everything that we already do. . . . I don't understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads."

Oracle's CEO 2008

CC represented not only a change in the way that business is done and IT resources are maintained more efficiently (Venters & Whitley 2012), it also changed the way the IT industry works, because *"nothing in IT lasts forever, and that technological evolution and economic factors can rapidly alter the trajectory of the industry."* (Campbell-Kelly 2009, p.30). As CC is a descendent model of IS/IT outsourcing, it is worth reviewing selectively the key areas related to the adoption of IS/IT outsourcing in the IS literature that will be discussed in the next section.

2.2 IS/IT Outsourcing Adoption Research

"The other part of outsourcing is this: it simply says where work can be done outside better than it can be done inside, we should do it." - Alphonso Jackson

Market demands are increasingly changing as IT advancements continue to emerge. Thus, organizations strive to become more agile in responding to market dynamics. They have to make challenging decisions in order to leverage the benefits of adopting IS/IT outsourcing practices (Dibbern et al. 2004). IS research into IS/IT outsourcing has focused on: (1) understanding and explaining IS/IT outsourcing decisions and their

impact on organizations, and (2) managing the relationship between the client and the vendor (Rivard & Aubert 2008; Hirschheim et al. 2007; Gonzalez et al. 2006).

Client organizations have drawn on several common arguments when deciding whether or not to adopt IS/IT outsourcing practices; in particular, they needed to focus on their core competencies and the reduction of IT costs (Hirschheim et al. 2007). Viewing IT as a cost rather than as a strategic niche has been interpreted in the literature as a "lack of understanding of IT value" (Lacity et al. 1994). Thereafter, several factors have appeared to influence IS/IT outsourcing decisions; these have included why (e.g., to reduce costs), what (e.g., selected non-core IS functions), which (e.g., offshoring or domestic outsourcer), and how (formal relationship management), and outcomes (e.g., met expectations, satisfaction, and performance quality) (Dibbern et al. 2004; Lacity et al. 2010). These factors are related to changes in the external business environment, and a client organization's internal environment, as well as the relationship between the two (Levina & Ross 2003; Loh & Venkatraman 1992b; Grover et al. 1996; Smith & Kumar 2004; Currie & Seltsikas 2001). Lacity et al. (2009) and Lacity et al. (2010) examined IS literature on various aspects of IS/IT outsourcing. They offered strong evidence that the likelihood of outsourcing IS/IT functions is determined by the case that a client organization is facing financial troubles. However, the lack of internal IT expertise may also determine the likelihood of outsourcing IS/IT functions (Jayatilaka et al. 2003; Lacity et al. 2010). Furthermore, the criticality and the level of customization or standardization of business processes are reported to determine the likelihood of outsourcing IS/IT functions (Huyskens & Loebbecke 2006). Additionally, the literature reported that firm size determines the likelihood of outsourcing IS/IT functions; however, the evidence is not clear, with some studies showing cases in which both large firms and small firms are likely to outsource IS/IT functions (Lacity et al. 2009).

Factors involved in making IS/IT outsourcing decisions include cost reduction and focus on core competencies, both of which are strong drivers of an organization's strategic intents to outsource IS/IT functions. This is in line with the findings of Hirschheim et al. (2007). Then, it is relatively clear that the desire to gain access to expertise and improve business processes drive the decision to outsource IS/IT functions. Furthermore, announcements of major IS/IT outsourcing decisions (e.g., Kodak (Loh & Venkatraman 1992b)) and competition (e.g., (Chen & Wu 2012)) have a strong influence on the intention to imitate the same decisions (Lacity et al. 2010). However, a study on IS/IT outsourcing from 1985 to 1995 found no effect of Kodak's

decision; rather, external media, vendor pressure, and internal communication on a personal level between managers in the companies had a significant influence on the decision to adopt IS/IT outsourcing (Hu et al. 1997).

Types of IS/IT outsourcing, whether selective or total, share common risks, such as the 11 client-centric risks identified by Earl (1996). These risks are: the possibility of weak management, inexperienced staff, business uncertainty, outdated technology skills, endemic uncertainty, hidden costs, lack of organizational learning, loss of innovative capacity, dangers of an eternal triangle, technology indivisibility, and fuzzy focus. Each type of IS/IT outsourcing risk (e.g., lack of prior outsourcing experience or poorly structured contracts) has its own mitigation strategies (Willcocks et al. 1999). Likewise, each IS/IT outsourcing type, including ASP, has its owns risks and mitigation strategies (Kern, Willcocks, et al. 2002). Contract design and standards are two ways to mitigate certain risks such as vendor opportunism (i.e., the vendor changes the contract or the vendor's staff misuse the client's data) and interoperability across vendors' products (i.e., vendor lock-in), which introduces unfavorable switching costs (Whitten & Wakefield 2006). Hence, data security and the risks associated with the loss of control have significantly influenced IS/IT outsourcing decisions (Lacity et al. 2010).

Further risks related to IS/IT outsourcing are technology development risks (Clemons & Chen 2011), which can be categorized into: (1) functionality risks, such as the extent to which it is difficult to integrate new applications with legacy systems, (2) political risks, such as staff resistance, because they feel their jobs are threatened by the IS/IT outsourcing arrangement, (3) technical risks, such as the case when the project exceeds the skills of existing IT staff, or the available hardware and software capabilities, and (4) financial risks, such as when the IS/IT outsourcing project fails to deliver the expected benefits.

The success of IS/IT outsourcing is determined by outsourcing decisions and the governance of the relationship between the client and the provider. The degree of outsourcing decisions determines the success of IS/IT outsourcing; hence, selective outsourcing decisions are likely to guarantee success. Furthermore, the role of top management's support for an IS/IT outsourcing decision increases the chance of success. Evaluating the supplier is a further determinant for IS/IT outsourcing success. This involves comparing prices and evaluating the vendor's credibility, financial viability, risks, and experience (Jayatilaka et al. 2003; Kern, Willcocks, et al. 2002).

The governance of the relationship between the client and the vendor can be either contractual or relational. Contractual governance includes contract details, type, duration, and size. A high degree of detail in a contract in terms of service levels, prices, warranties, and penalties indicates a good contractual governance practice that leads to successful IS/IT outsourcing. Type of contract (e.g., fixed fee-for-service) is also considered a success factor in IS/IT outsourcing. Lacity and Willcocks (1998) found that the following types of contracts are attractive to clients: flexibly-priced contracts, performance-based contracts, and partnership contracts that are based on shared risks and rewards. Furthermore, the flexibility of contracts in terms of enabling the client to switch from one vendor to another is deemed to be favorable (Benaroch et al. 2010). Contract duration (e.g., long-term or short-term) and size (in dollars) also contribute to IS/IT outsourcing success. Short-term contracts are deemed to be more successful than long-term contracts (Lacity et al. 1996). Large contracts indicate that vendors are willing to provide a high quality service, which can lead to a successful IS/IT outsourcing arrangement. Furthermore, contract misalignment with the client organization's needs is deemed to negatively impact on the survival of the vendor; thus, contracts should be well-structured to minimize agency costs (Susarla & Barua 2011).

Once an organization has entered into an IS/IT outsourcing arrangement, managing its relationship with the vendor becomes crucial; thus, the literature has asserted the importance of the outsourcing relationship and its evolution over time (Kern & Willcocks 2000). This relationship has to be focused on achieving the client's objectives and the performance of the vendor towards achieving these objectives (Kern & Willcocks 2000). Relational governance is one way of maintaining this relationship, through the management of trust, norms, open communication, information sharing, mutual dependency, service quality, and cooperation (Sabherwal 1999; Grover et al. 1996; Lee & Kim 1999; Mathew & Chen 2013; Benlian et al. 2011). Contractual governance and relational governance complement each other in terms of a well-structured SLA that leverages relational governance. At the same time, a change in the SLA's characteristics has been shown to negatively influence trust (Goo et al. 2009). Furthermore, a client's prior experience and expectations of vendor performance resulting from similar IS/IT outsourcing practices are also important for maintaining an IS/IT outsourcing arrangement (Susarla et al. 2003).

Lacity et al. (2010) extensively reviewed the literature on IS/IT outsourcing research and explored more areas related to IS/IT outsourcing decisions and outcomes than

those given above. Thus, the authors suggested the need for further research endeavors towards exploring more IS/IT outsourcing-related areas such as strategic motivations and emerging models such as CC.

2.3 Cloud Computing As An Emerging IS/IT Outsourcing Model

"If you think you've seen this movie before, you are right. Cloud computing is based on the time-sharing model we leveraged years ago before we could afford our own computers. The idea is to share computing power among many companies and people, thereby reducing the cost of that computing power to those who leverage it. The value of time share and the core value of cloud computing are pretty much the same, only the resources these days are much better and more cost effective. Moreover, you can mix and match them to form solutions, which were not possible with the traditional time-sharing model."

- David Linthicum (2010, p.8)

The definition of the CC model put forward by NIST is widely used. According to NIST, CC is *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance 2011, p.2). By definition, CC offers the capability of a flexible IT infrastructure that aligns IT with business needs (Duncan 1995). NIST has further described the five characteristics of CC model: (1) on-demand self-service: where the client organization can automatically self-provision computing capabilities as needed without human interaction with the CSP; (2) broad network access: where computing capabilities are made accessible over the network by heterogeneous client platforms; (3) resource pooling: where the CSP's physical and virtual computing resources (i.e., storage, processing, memory, and network bandwidth) are pooled and utilized by multi-tenants, who can only know the location of the datacenter, but not the location of the VM being utilized in the cloud environment; (4) rapid elasticity: where computing capabilities can be scaled in and out automatically whenever needed; and (5) measured service: where the cloud systems automatically monitor, control, optimize, and report the usage of resources; thus, providing transparency for CSPs and clients.

These five characteristics exist in three basic CC service models (Mell & Grance 2011; Hogan et al. 2011): (1) SaaS model: where application capabilities are made accessible

to clients through a web browser with limited configurations. (1) SaaS model: where application capabilities are made accessible to clients through a web browser with limited configurations. Clients do not have to manage and control the cloud infrastructure; (2) PaaS model: where clients are provided with the capability to deploy applications created by the client onto the CSP's infrastructure. They can also use the CSP's programming libraries and tools to create and deploy applications with limited configurations on the cloud deployment environment; and (3) IaaS model: where clients are provided with the capability to provision IT infrastructure resources (i.e., processing, storage, networks, and computing power) to deploy and run operating systems and applications. With the IaaS model, clients have limited control over network components.

CC service models can be deployed on four types of cloud, depending on the sensitivity of data and applications: private, public, community, and hybrid clouds (Mell & Grance 2011). The only typical scenario for a public cloud is that the cloud infrastructure is managed by, owned by, and located within the CSP. Private and community clouds are often considered to be based on the same core idea: a private cloud is provisioned by a single client organization (SOC), whilst community clouds are private clouds provisioned by a community of client organizations (CCO) that share common concerns. There are eight possible, but similar, scenarios for each of these cloud types. Hybrid clouds are a mix of public cloud and internal private cloud or legacy systems. Scenarios for hybrid clouds involve both SOC and CSP throughout. Table 1 presents scenarios for the deployment of CC services, taken from a report by CSA about critical areas of cloud security (CSA 2009).

Table 1: Scenarios for deploying CC services (adapted from CSA, 2009)

	Infrastructure management			**Infrastructure ownership**			**Infrastructure location**	
	SCO	**CCO**	**CSP**	**SCO**	**CCO**	**CSP**	**Client's on-premise**	**Client's off-premise**
Public			x			x		x
Private	x			x			x	
	x			x				x
	x					x	x	
	x					x		x
			x	x			x	
			x	x				x
			x			x	x	
			x			x		x
Community		x			x		x	
		x			x			x
		x				x	x	
		x				x		x

	Infrastructure management			Infrastructure ownership			Infrastructure location	
	SCO	**CCO**	**CSP**	**SCO**	**CCO**	**CSP**	**Client's on-premise**	**Client's off-premise**
			x		x		x	
			x		x			x
			x			x	x	
			x			x		x
Hybrid	x		x	x		x	x	x

CC models have changed the way that organizations handle data and IT resources (Najjar & Kettinger 2013). In particular, they offer strategic capabilities (e.g., scalability, ubiquity, and mobility) to organizations that would not normally be available in-house (Iyer & Henderson 2010; Venters & Whitley 2012). These capabilities bring benefits to organizations, such as innovation through increased business focus, increased efficiency in work, and rapid response to dynamic market demands (Iyer & Henderson 2012). CC is argued to be a new emerging IS/IT outsourcing model that shares the same principles, benefits, and risks as IS/IT outsourcing (Schneider & Sunyaev 2014; Lacity et al. 2010). Nonetheless, CC has its own characteristics in terms of shifting responsibilities, advanced governance approaches, and the acquisition of on-demand self-service standard services that are contracted on a short-term pay-per-use basis (Schneider & Sunyaev 2014). Although CC models resemble the utility model for electricity, it would not be fair to oversimplify the situation and consider CC services in the same way as electrons:

"If the utility model were adequate, the challenges to cloud computing could be solved with electricity-like solutions—but they cannot. The reality is that cloud computing cannot achieve the plug-and-play simplicity of electricity, at least, not as long as the pace of innovation, both within cloud computing itself, and in the myriad applications and business models it enables, continues at such a rapid pace…..Firms that simply replace corporate resources with cloud computing, while changing nothing else, are doomed to miss the full benefits of the new technology….. It is true that this inevitably requires more creativity and skill from IT and business executives. In the end, this is not something to be avoided. It should be welcomed and embraced."

(Brynjolfsson et al. 2010, p.34)

Typically, CC represents a shift in the responsibilities of maintaining, upgrading, and even securing IS/IT from the client to the CSP. Such a shift poses risks (e.g., breaching data confidentiality, integrity, and availability); indeed, benefits can even turn into

risks (Venters & Whitley 2012; Marston et al. 2011; Neumann 2014; Ryan 2011). Hence, at some point in time, the criticality of data and applications will dictate whether or not they are maintained in-house, because they require more security audits, fault-tolerant network performance, and/or are high-volume generating transaction systems (Brynjolfsson et al. 2010). Thus, it is a matter of being selective when deciding to adopt CC services. The maturity of the internal enterprise IT architecture must also be taken into consideration (Schneider & Sunyaev 2014; Marston et al. 2011; Xin & Levina 2008).

On the whole, client organizations choose to adopt CC services so that they can focus more on their core competencies and cost reduction (Garrison et al. 2012); likewise, these are typical motivations for IS/IT outsourcing. However, there is a risk that client organizations lose the ability to evaluate the CSPs and, in some situations, the matter of responsibilities can become blurred (Venters & Whitley 2012). CC models share the same risks as IS/IT outsourcing (as outlined in Section 2.2), including *legislative risk* (Clemons & Chen 2011). Indeed, this risk is specific to CC models in that it is related to storing data in geographically dispersed data centers, which can complicate and blur the responsibilities for securing data (Seddon & Currie 2013; Neumann 2014; Ismail 2011). The legal issues may include conflict between local and international laws, because some countries or regions have strict laws regarding data privacy, whilst others have weak or non-existent laws (Marston et al. 2011; Ismail 2011). Furthermore, global US-based CSPs may lose the trust of clients should the US authorities accidentally seize their data under the Patriot Act (Venters & Whitley 2012; Kshetri & Murugesan 2013; Kshetri 2013). For some clients, such as government agencies (Paquette et al. 2010), more security restrictions are demanded (Desai 2013); for example, global CSPs may need to comply with the Safe Harbor agreement (Seddon & Currie 2013; Ismail 2011). Data protection laws vary from one country to another; they may not fit a CC model. In this case, new laws may need to be fashioned (Desai 2013).

Although the risk of vendor lock-in is still applicable to CC models, it is only likely to happen with SaaS and PaaS service models, and not with the IaaS model (Clemons & Chen 2011; Armbrust et al. 2010). Interoperability among cloud-based software providers is a further concern, because of a current lack of supporting standards (Marston et al. 2011; Malladi & Krishnan 2012). Thus, it is necessary to speed up the development of standards in order to make the movement of data and applications between CSPs easier and cheaper (Kshetri 2013). To date, only major CSPs such as

Google and Salesforce have maintained APIs that allow the integration of product features from each other (Cusumano 2010; Iyer & Henderson 2010); however, this is not the case with all CSPs, making the selection of CSPs even harder (Mcgeogh & Donnellan 2013). Vendor lock-in risk affects the availability of data, either when switching from one CSP to another or when sharing data with business partners who use CC services offered by different CSPs (Seddon & Currie 2013). Such a risk may have to be accepted and dealt with in a trade-off sense (Creeger 2008); *"Depending on the application, its engineering, and its intended use, cloud offerings will not be interchangeable across cloud providers."* (Brynjolfsson et al. 2010, p.34).

Furthermore, when CSPs subcontract part of their services to third party providers, this raises additional security and legal concerns to those found in traditional IS/IT outsourcing scenarios (Jansen 2011; Heiser & Nicolett 2008). This gave rise to a new governance approach called *participatory governance*, which is defined as "the distribution of decision rights across multiple internal and external participants" (Andriole 2015, p.54). Internal participants include corporate leaders, business functions, and business units. External participants are hardware and software providers, business partners and suppliers, and any other external parties, including regulatory bodies or standards associations in some cases (Alshamaila & Papagiannidis 2013; Andriole 2015; Kshetri 2013). This form of governance has emerged alongside CC models; indeed, it did not exist in prior IS/IT outsourcing models. It is supported by certifications to ensure that CC services fulfill pre-set criteria by the client organization to mitigate risks and uncertainties (Lansing et al. 2013).

The notion of *on-demand self-service standard services and shared environment* gives rise to both benefits and risks. The on-demand self-service characteristics of CC model are offered through elasticity; indeed, it is considered to be *"the true golden nugget of CC and what makes the entire concept extraordinarily evolutionary, if not revolutionary"* (Owens 2010, p.46). Elasticity is achieved through the virtualization of IT resources, which enables client organizations to access computing resources in the form of VMs at any time, as needed, instead of buying hardware and waiting for its configuration. Thus, the benefits include cost savings and efficiency (Kotsovinos 2011). However, virtualization is not enough to fully describe the CC model; it also has to use a high degree of automation to acquire the shared IT resources in the CC environment (Durkee 2010).

Despite the benefits brought by virtualization, the CC environment is vulnerable because it is 'shared'. The hypervisor, which is the component responsible for creating and managing the VMs, can be compromised, leading to unauthorized access to other clients' VMs who share the same CC environment that is managed by the same hypervisor (Owens 2010; Cusumano 2010). This vulnerability poses a challenge to CSPs as they have to carefully segregate the VMs, define a set of fine-grained access controls over the entire virtual environment (i.e., who can access what and when), and provide transparent audit trails for legal compliance (Owens 2010). On the other hand, it is argued that CSPs have the technical expertise and capabilities to improve their CC security solutions; hence, virtualization becomes a solution to CC security problems instead of being part of them (Anthes 2010).

The 'shared environment' aspect of the CC model may leave it vulnerable, but at the same time, it is considered to be highly innovative (Su et al. 2009; Owens 2010). A shared environment of standard services can offer cost savings, flexibility, and agility; however, it does give rise to some complexity and limited customizability issues (Su et al. 2009). Furthermore, the shared IT environment of CC can pose performance issues if one of the tenants disrupts the service for others tenants who share the same IT resource. Such an incident is called DoS attack (Armbrust et al. 2010; Cusumano 2010). Existing literature has reported that previous IS/IT outsourcing models offered more customization than CC services because CC services are more standardized and shared so as to serve multiple clients (Schneider & Sunyaev 2014). It should be noted that public CC services are typically standardized, unlike those implemented privately by the client organization (Leavitt 2013).

However, each CC deployment model serves a particular situation. Private clouds are implemented internally; they are secure, customizable, and available without Internet connection. Thus, private clouds eliminate dependency on an external CSP (Leavitt 2013). Public CC services are appropriate for dynamic usage patterns and peak workloads. They avoid having to finance expensive hardware and software (Leavitt 2013). Hybrid CC services "combine the public cloud's cost savings and elasticity—enabling the on-demand acquisition and release of resources based on temporary needs without having to acquire additional infrastructure— with a private cloud's security, control, and customization." (Leavitt 2013, p.15). CC models still pose network latency issues (Armbrust et al. 2010); however, research efforts are in progress to optimize such a drawback (Nedbal et al. 2014).

The short-term pay-per-use feature of public CC services in particular makes them attractive to client organizations, because they do not need make large upfront investments into dedicated hardware and software (Durkee 2010). They only pay for the IT resources they use, which are offered by the CSP to allow them to cope with peak times. Problems may arise, however, including the occurrence of unpredicted costs as a result of increased use. Elasticity problems, such as scaling out, may also occur (Borgman et al. 2013; Schneider & Sunyaev 2014; Venters & Whitley 2012). Choosing a CSP based on the lowest price-per-use may also be at the expense of desired quality performance. In the sphere of 'perfect competition', some CSPs try to offer lower price CC services than those are offered by well-established CSPs. To offer such discounts, it may be necessary to cut corners on their infrastructure (Durkee 2010). Thus, unpredictable performance issues are likely to occur.

The SLA is one good tool for dealing with performance issues, although it is claimed itself to have issues: *"In the cloud market space, meaningful SLAs are few and far between, and even when a vendor does have one, most of the time it is toothless"* (Durkee 2010, p.65). SLAs for public CC services are weak in terms of availability, performance measures and guarantees; small penalties may also be applied (Lango 2014). To benefit from CC services, SLAs have to be negotiated with acceptable service levels in mind. Clients must also ensure clarity to avoid the risk of vendor opportunism. On the other hand, CSPs have to be transparent, and provide measures of the CC service's performance, security controls, and the true cost of using that service (Durkee 2010; Lango 2014). Transparency builds a client's trust in the expected performance of the service and the CSP (Garrison et al. 2012; Durkee 2010).

Trust as a relational capability is considered a 'strong' success factor for CC adoption, in addition to managerial and technical capabilities (Garrison et al. 2012). Trust results from the client organization's belief that the CSP has enough expertise and capabilities to offer the CC services as expected. Managerial capabilities relate to the role of the client organization's IT managers in facilitating the adoption of CC services (e.g., integrating CC services with legacy systems). Particularly important are their orchestration skills and experience. Technical capabilities imply the ability to respond quickly to ever-changing market demands by utilizing flexible and scalable CC services. However, to fully realize the benefits of adopting CC services, practice-based IS literature has suggested that client organizations should: (1) educate stakeholders about security in the cloud, (2) launch adoption gradually, giving proof of the concept of CC services, (3) match CC services to current business needs, (4) find the right CSP

by asking for referrals, by evaluating CSPs already known personally, and by renewing existing CSPs, (5) have an informal relationship with CSPs in addition to the formal relationship, and finally (6) acquire any skills needed by hiring CIOs with CC experience and IT professionals with CC orchestration skills (Lacity & Reynolds 2014). Furthermore, any organization considering CC adoption should consider assessing their current capabilities, together with any potential costs. Also key to a successful CC adoption strategy are: experimenting with CC services, having an SOA way of organizing information as services, clearly identifying access controls, and assuring compliance with regulations and corporate policies (Iyer & Henderson 2012; Iyer & Henderson 2010; Loebbecke et al. 2012).

The adoption of CC services is influenced by several internal, external, and technological factors (Morgan & Conboy 2013); these factors, to some extent, are also applicable to IS/IT outsourcing (Schneider & Sunyaev 2014). Empirically, these factors are reported in the literature as either positive influences, negative influences, or desires (Schneider & Sunyaev 2014; Venters & Whitley 2012). Examples of technological factors include the perceived complexity of legacy systems and security in terms of losing control and availability. Perceived complexity, security, and availability are reported to have a negative influence on the adoption of IS/IT outsourcing in general and CC in particular (Lacity et al. 2010; Schneider & Sunyaev 2014). An example of an internal factor is top management support. Top management support is reported to have a positive influence on the adoption of IS/IT outsourcing and CC (Schneider & Sunyaev 2014; Lacity et al. 2010). An example of an environmental factor is market maturity in terms of legal, technological, and vendor maturity. The IS/IT outsourcing market is reported to be more mature than the CC market; however, market maturity is likely to have a positive influence on the adoption of both IS/IT outsourcing and CC (Schneider & Sunyaev 2014). In the next Section, I present CC adoption factors that have been identified in a systematic review of existing literature. In addition, I introduce the method used to conduct this literature review. Finally, I discuss the key findings and implications that have motivated me to take certain theoretical, methodological, and empirical research directions.

2.4 A Systematic Literature Review on Cloud Computing Adoption Research

Regarding CC in particular, I conducted a systematic review of existing literature (cf. Paper2) to identify the factors that influence the adoption of CC services in

organizations, as well as the areas that have been researched with regard to the adoption processes (El-Gazzar 2014). Reviewing the literature is an essential process that facilitates the identification of areas in which more research is needed (Webster & Watson 2002). This review process followed fundamental guidelines for conducting an effective literature review (Webster & Watson 2002; vom Brocke et al. 2009; Levy & Ellis 2006), and was carried out within certain boundaries (Webster & Watson 2002). The contextual boundary was the enterprise users; there are significant issues that need to be addressed before they can use CC services (Marston et al. 2011; Dubey & Wagle 2007). The temporal boundary of this review covers the published articles in all years before February 2014. The literature search process of this review involved querying seven quality scholarly literature databases (AISeL, IEEE Xplore, ScienceDirect, EBSCOhost, ProQuest, Wiley online library, and ACM digital library). These databases allowed me to access leading IS journals and high-quality peer-reviewed IS conference publications (Levy & Ellis 2006). Furthermore, online databases are appropriate and practical sources for reviewing the literature about a contemporary phenomenon such as CC (Yang & Tate 2012). The search criterion was limited to paper titles in order to ensure their relevance. The terms used for searching all seven databases were CC in combination with *adopt** and other related terms, such as *accept** and *diffuse**. This initially resulted in 94 papers.

The practical screening process involved reading the abstract of these papers to decide whether or not they were relevant to this review (vom Brocke et al. 2009; Okoli & Schabram 2010). Furthermore, the filtering criteria involved the exclusion of recurring papers, research-in-progress papers, non-English language papers, those with a focus on individuals, and periodical articles published by news websites, trade journals, and magazines. These exclusion criteria delimit the sample of papers so that the literature review is practically manageable (Okoli & Schabram 2010). This screening process resulted in 51 papers for the classification.

The reviewed papers were classified according to the research methods used in them to determine the extent of CC adoption research (Orlikowski & Baroudi 1991; Galliers & Land 1987; Gonzalez & Dahanayake 2007). The research methods used in the reviewed papers included laboratory experiments, field studies, the Delphi study, interviews, literature reviews, case studies, and surveys. Some papers did not have a methodology section and they reflect on some concepts in relation to CC (e.g., cost, security, performance, etc.) or they adopt theories without empirical testing. I labeled these papers as “conceptual papers”. Classification of the 51 articles involved using a

bottom-up grounded theory (GT) approach (Glaser & Strauss 1967). The GT approach is said to be valuable for conducting a rigorous literature review (Wolfswinkel et al. 2011), "instead of force-fitting the data to an a priori theory" (Rich 2012, p.3). The 51 reviewed papers were classified according to a GT approach to "reach a thorough and theoretically relevant analysis of a topic" as suggested by Wolfswinkel et al. (2011, p.1). The classification process resulted in 30 labeled concepts from open coding. Axial coding resulted in grouping the 30 concepts into eight corresponding categories (i.e., internal, external, evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation). Finally, selective coding was applied to integrate and refine the eight main categories and to develop relationships between them (Wolfswinkel et al. 2011). This resulted in two abstract categories: cloud adoption factors (i.e., internal and external) and cloud adoption processes (i.e., evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation). These are shown in Figure 4, together with the distribution of studies among the factors. Three factors were predominantly recurring in the reviewed papers: government regulations as an external factor, top management influence as an internal factor, and perceived risks and benefits as an adoption processes-related factor. Based on my review's findings, I discuss these three factors in the paragraphs that follow.

Government regulations are found to ensure secure adoption of CC; however, the inconsistency or lack of regulations across countries is likely to be an obstacle for adopting CC services. Furthermore, regulations such as the Sarbanes-Oxley Act (SOX) for corporate accounting data, the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA) were enacted before CC was becoming increasingly adopted; thus, they might not be sufficient to facilitate its adoption (Kim et al. 2009; Kushida et al. 2011). However, some countries started to enact laws specific to CC, such as the *cloud first policy* and the Health Information Technology for Economic and Clinical Health (HITECH) Act in the USA and the *cloud computing strategy* introduced by the Australian government (Bhat 2013; Kushida et al. 2011). The inconsistency of international government regulations is a further concern, because there is no widely agreed data privacy policy among all governments (Kushida et al. 2011).

Some countries restrict enterprises to only storing their data in a CC infrastructure within their national borders (Jensen et al. 2011). For instance, the EU's privacy laws prohibit the exchange of personal information outside the users' jurisdiction (Mcgeogh

& Donnellan 2013). This is because CSPs that operate outside of their home country must comply with the host country's regulations and government surveillance, a ruling that some enterprises may find it difficult to comply with (Bhat 2013; Abokhodair et al. 2012). An example of the multi-jurisdictional politics that can have a negative impact on CC adoption is the USA Patriot Act, which makes countries, especially those within the EU, skeptical about dealing with US-based CSPs (Avram 2014; Kushida et al. 2011). However, some CSPs have solved this issue by allowing enterprises to deploy their IT resources on physical servers located within the EU region (Avram 2014). Thus, in the developed world, although government regulations are in place, they often conflict with each other. In the developing world, they are not adequately placed at all (Bhat 2013; Kushida et al. 2011).

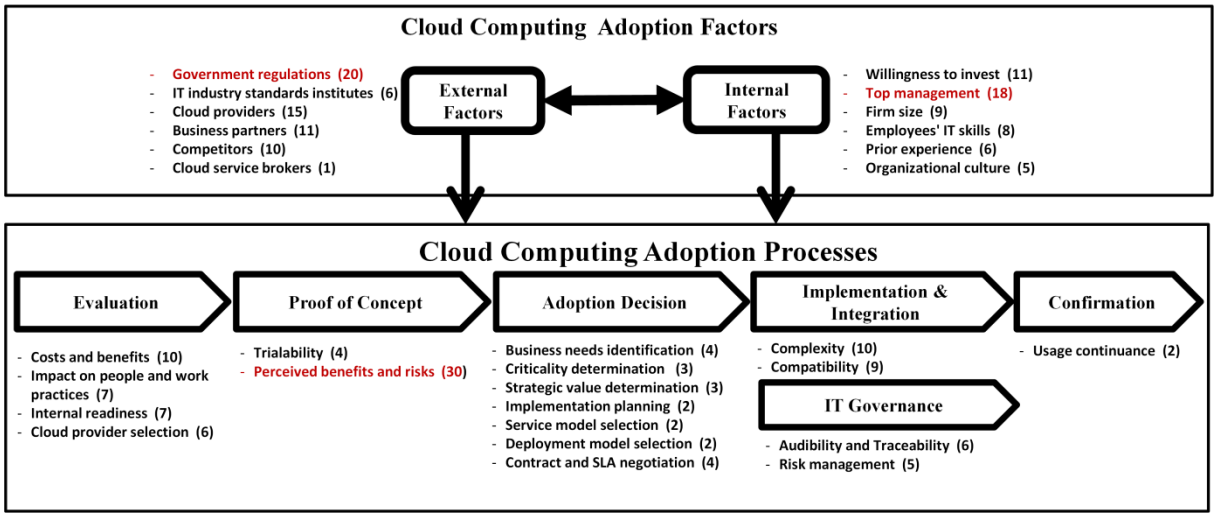


Figure 3: Cloud computing adoption factors and processes (Paper2)

A cornerstone to the adoption of CC is the IT knowledge, competence, and capability that top management contributes to creating a suitable organizational climate. Such a climate must offer an adequate budget, sufficient human and IT resources, and enough time (Bharadwaj & Lal 2012; Borgman et al. 2013; Alshamaila & Papagiannidis 2013; Lian et al. 2014). This involves: (1) understanding CC and its architecture, service models, and strategic values (Nasir & Niazi 2011; Luoma & Nyberg 2011; Espadanal & Oliveira 2012; Rawal 2011; Rath et al. 2012; Misra & Mondal 2011); (2) identifying an enterprise's business needs and aligning IT decisions with business strategies (Mcgeogh & Donnellan 2013; Subramanian 2012); (3) evaluating the readiness of the existing IT infrastructure, IT knowledge, and human resource skills, available resources, and culture (Rath et al. 2012; Luoma & Nyberg 2011; Borgman et al. 2013; Espadanal & Oliveira 2012); and (4) steering towards CC adoption (e.g.,

deciding on an adoption strategy, governance of integration and implementation, and evaluation of CC services after use) with the guidance of external regulatory and professional bodies (Morgan & Conboy 2013; Mcgeogh & Donnellan 2013).

There is a wide agreement on the significant influence of the perceived benefits and risks related to the adoption of CC services (Alshamaila & Papagiannidis 2013; Iyer et al. 2013). This viewpoint is consistent with the findings of a survey that found the management's perceptions of security, cost-effectiveness, and IT compliance to have a significant impact on the decision to adopt CC (Opala & Rahman 2013). These benefits include cost savings, agility, flexibility, ease of use, scalability, the ease of collaboration between business partners, less operational effort on the part of CIOs, and increased productivity (Borgman et al. 2013; Malladi & Krishnan 2012; Bharadwaj & Lal 2012; Nkhoma et al. 2013; Lin & N.-C. Chen 2012; Subramanian 2012; Gupta et al. 2013). However, by proofing concept of CC services, enterprises should be able to identify risks and benefits so that they can decide whether or not to adopt CC. The identified risks in this review include (Onwudebelu & Chukuka 2012; Jensen et al. 2011; Nkhoma et al. 2013; Lin & N.-C. Chen 2012; Nuseibeh 2011; Iyer et al. 2013; Avram 2014):

- Organizational risks, which cover the risk of vendor lock-in as well as the loss of governance within the enterprise.
- Technical risks, which include data leakage, loss of data, downtime, data bottlenecks, and cyber-attacks.
- Legal risks, which include data protection regulations and licensing issues.
- Nontechnical risks, which refer to the misuse of cloud services and natural disasters.
- Performance risks, which primarily result from the moving of huge amounts of data to cloud servers. This movement can take a long time and, when moving further in the adoption, it will require increasing bandwidth and connectivity, which is costly (Morgan & Conboy 2013).

The above discussed empirical findings are one outcome from my systematic review. Next, I discuss methodological and theoretical findings. In the 51 reviewed papers, research methods were identified: Lab Experiment (LE) = one paper, Field Study (FS) = two papers, Case Study (CS) = six papers, Delphi Study (DS) = two papers, Survey (SUR) = 24 papers, Interviews (INT) = four papers, Conceptual Paper (CP) = 17

papers, Literature Review (LR) = one paper. The methodological findings indicate that fewer qualitative studies (e.g., case studies, interviews, and field studies) have contributed to the understanding of CC adoption factors and processes compared with quantitative studies (e.g., surveys). In some papers, multiple methods are used (Cegielski et al. 2012; Shin et al. 2013; Borgman et al. 2013; Tjikongo & Uys 2013). Furthermore, external adoption factors are extensively addressed by surveys and conceptual papers, and less addressed by in-depth qualitative studies. This applies similarly to internal factors. In general, adoption processes, such as evaluation, adoption decision, implementation and integration, IT governance, and confirmation, are not adequately addressed, except for the proof of concept process.

The review indicates the need to conduct multiple qualitative case studies in different contexts (e.g., countries and industries) if we are to gain a better understanding of CC adoption factors and processes. Hence, there is a need for interpretive case studies to investigate each of the factors and processes found during this review (e.g., willingness, organizational culture, regulations, trustworthiness of CSPs, evaluation of CC services, adoption decision, and implementation and integration processes). Such in-depth studies are preferred, because of their implications for both practice and academia (Walsham 1995).

When considering CC, enterprises must make a decisive choice between in-house and on-demand approaches. In this regard, the Delphi method can help IT managers to identify the most important issues and priorities that should be considered when deciding to adopt CC solutions (Dalkey 1972; Okoli & Pawlowski 2004; Hsu & Sandford 2007). The Delphi method was rarely used in the reviewed papers. Furthermore, this review advocates the need for conducting longitudinal studies to assess the impact of CC implementation on both the technical and managerial capabilities of an enterprise (e.g., integration with existing IT infrastructure, planning, risk management, and IT governance) as well as the impact of the confirmation process on organizational innovation.

The theoretical findings from the 51 papers are organized according to the theory, framework or model used. Some papers discuss related concepts (e.g., performance, cost, security, or CSPs); thus, they are considered to use “general concepts”. Other papers have taken a GT approach to understanding CC adoption, basing their models on field data. Papers that tested theories empirically using field data are predominant, although non-empirically tested theoretical contributions are also much in evidence.

On the whole, general concepts were most frequently used to explain CC adoption factors and processes. The technology-organization-environment (TOE) framework was also more frequently used compared with other theories. Diffusion of innovation (DOI) theory and the GT approach appear to be the next most frequently used frameworks in the reviewed papers. Empirically tested theories/frameworks/models are also dominant with 34 papers, whereas studies with no empirical testing were less common: 17 papers. However, the number of studies that did not use empirical testing is not negligible, which suggests that more field work is needed. Furthermore, the majority of papers used a combination of multiple theoretical perspectives to gain more insights into CC adoption factors and processes.

Hence, more theories need to be applied (e.g., institutional theory (Mignerat & Rivard 2009; Weerakkody et al. 2009)) if we are to gain a greater insight into CC adoption. Institutional theory captures the notion of irrationality in decision making or, in other words, a legitimacy-motivated decision-making. For example, an enterprise may or may not adopt CC because of internal (e.g., cultural resistance and internal readiness) or external pressures (e.g., competitors and business partners), rather than because of increased efficiency and cost reduction. Moreover, institutional theory is helpful in understanding how and why enterprises respond to external and internal pressures (Oliver 1991; Deephouse & Suchman 2008). Consequently, this review raises several interesting questions for IS researchers engaged in empirical investigation: for example, what factors (i.e., internal and external) can affect the adoption of CC, and how do enterprises form strategies to cope with these factors?

In the next chapter, I put forward the arguments for using a theoretical foundation as an analytical lens for my research. In particular, I elaborate on the reasons for choosing neo-institutional theory, its role in my research, its use in IS research in general, its nature, and the concepts used in my study (i.e., Isomorphic pressures and strategic responses). I go on to discuss the institutional influences that have appeared in IS literature. These influences play a role in facilitating, constraining, or even hindering the adoption of IS/IT outsourcing and CC.

2.5 Summary of the Chapter

In this chapter, I have provided an overview of the IS/IT outsourcing models that emerged over time, finally becoming the CC model we know today. I discussed the IS research stream with regard to the adoption of IS/IT outsourcing and the IS research stream with regard to the adoption of CC. A comparison between IS/IT outsourcing

and CC was also made. Finally, I discussed the key findings from my second paper (Paper2), which provided a systematic review of the existing literature on CC adoption and any research gaps (i.e., theoretical, methodological, and empirical).

“Theory helps us to bear our ignorance of fact.”

— George Santayana

3 Theoretical Foundation

In this chapter, I elaborate on the theoretical foundation for my research. In Section 3.1, I argue for choosing neo-institutional theory as an analytical lens for the data collected and introduce the theoretical concepts used in my research. In Section 3.2, I review existing IS research, including IS/IT outsourcing, with regard to the use of neo-institutional theory. In Section 3.3, I review research stream in the area of CC in which neo-institutional theory has been used. Finally, in Section 3.4, I offer a summary of the chapter.

3.1. Neo-Institutional Theory

The choice and application of theories is an essential, if somewhat challenging, process for the researcher: *"If we talk of what is known and what is unknown, we may be referring to the presence or absence of the data to corroborate our theories, or to the inability of our theories to provide meaning to the curious phenomena we observe and measure."* (Diebold et al. 2010, p.2). Furthermore, theory can be used at different stages of the research, either as a guide for data collection or data analysis or, as is sometimes the case, as a final product of the research (Walsham 1995). However, the choice of theory is subject to the researcher's experience, background, and interests (Walsham 2006). My choice of neo-institutional theory for the analysis phase is based on the feeling that it is *"insightful";* it inspires me to gain a better insight into my field data, as advised by Walsham (2006, p.325). Neo-institutional theory belongs to type IV theory in Gregor's (2006) taxonomy, which is a theory used to explain and predict (EP).

I have used neo-institutional theory to explain, because, *"explanation is closely linked to human understanding, as an explanation can be provided with the intent of inducing a subjective state of understanding in an individual."* (Gregor 2006, p.617). In doing so, I used the data-theory link on data extracted from the interviews to identify further facts and gain a good insight into the factors that influence the adoption of CC. In particular, I chose the concept of isomorphic pressures (DiMaggio & Powell 1983) and strategic responses to these isomorphic pressures (Oliver 1991). Isomorphic pressures helped me understand why organizations adopt similar practices, such as CC, whilst the strategic responses helped me to better understand how organizations respond to these pressures in order to maintain their legitimacy (DiMaggio & Powell 1983; Oliver 1991; Suchman 1995).

Furthermore, neo-institutional theory demonstrates the notion of irrationality in decision-making, which drives organizations to seek *legitimacy* more than efficiency (Avgerou 2000; Orlikowski & Barley 2001; Mignerat & Rivard 2009). Legitimacy is defined as the *"congruence between the social values associated with or implied by [organizational] activities and the norms of acceptable behavior in the larger social system"* (Dowling & Pfeffer 1975, p.122). Legitimacy is gained when organizations are required to unquestioningly accept and follow rules and social norms, that are enacted at the *organizational field level* (Tolbert & Zucker 1996; Wooten & Hoffman 2008).

The organizational field level is a central concept in neo-institutional theory, and can be defined as *"a community of organizations that partakes of a common meaning system and whose participants interact more frequently and fatefully with one another than with actors outside the field"* (Scott 2001, p.84). This may include regulatory bodies, business partners (e.g., customers and suppliers), peer organizations, competitors, and professional and trade associations. Institutions are socially constructed by social, political, economic, and legal contexts (i.e., organizational field or institutional environment), which enact the rules and norms of accepted social behavior for either individuals or organizations (Weerakkody et al. 2009). These contexts exert isomorphic pressures on organizations, requiring them to conform to these rules and norms in order to gain legitimacy (Weerakkody et al. 2009). Institutions are defined as:

"Social structures that have attained a high degree of resilience. [They] are composed of cultural-cognitive, normative, and regulative elements that, together with associated activities and resources, provide stability and meaning to social life. Institutions are transmitted by various types of carriers, including symbolic systems, relational systems, routines, and artifacts. Institutions operate at different levels of jurisdiction, from the world system to localized interpersonal relationships. Institutions by definition connote stability but are subject to change processes, both incremental and discontinuous" (Scott 2001, p.48).

Isomorphism is experienced by organizations through the exertion of three pressures (i.e., coercive, normative, and mimetic); these are illustrated in Table 2. It can be argued that these pressures overlap empirically, although they are caused by different circumstances and lead to different outcomes (DiMaggio & Powell 1983). Isomorphic

pressures exist when *connectedness* happens, which is the exchange of relations between organizations.

Table 2: Isomorphic pressures (DiMaggio & Powell 1983)

Isomorphic pressure	Description
Coercive	Imposed by the legal environment and can be either formal (e.g., laws and standards) or informal (e.g., cultural)
Normative	Imposed by professional associations that define normative rules about organizational and professional behavior. Likewise, universities and professional training institutions produce individuals with similar orientations and educational backgrounds.
Mimetic	Imposed by environment uncertainties (e.g., goal ambiguity or poor awareness of organizational innovation), so that organizations model themselves on other successful organizations in their field

Undoubtedly, *"early adoption decisions of organizational innovations are commonly driven by a desire to improve performance"* (DiMaggio & Powell 1983, p.148). However, as innovations diffuse, an adoption decision may become driven more by the desire to achieve legitimacy (Meyer & Rowan 1977). In order to gain legitimacy, organizations implement five strategic responses through a set of tactics to respond to isomorphic pressures (Oliver 1991), as illustrated by Table 3.

Table 3: Strategic responses to institutional processes (Oliver 1991)

Strategic responses	Tactics	Examples
Acquiescence	Habit	Following invisible, taken-for-granted norms
	Imitate	Mimicking institutional models
	Comply	Obeying rules and accepting norms
Compromise	Balance	Balancing the expectations of multiple constituents
	Pacify	Placating and accommodating institutional elements
	Bargain	Negotiating with institutional stakeholders
Avoidance	Conceal	Disguising nonconformity
	Buffer	Loosening institutional attachments
	Escape	Changing goals, activities, or domains
Defiance	Dismiss	Ignoring explicit norms and values
	Challenge	Contesting rules and requirements
	Attack	Assaulting the sources of institutional pressure
Manipulation	Co-opt	Importing influential constituents
	Influence	Shaping values and criteria
	Control	Dominating institutional constituents and processes

From a social science perspective, neo-institutional theory has its origins, and has been used in research, in various disciplines, including economics, political science, organization science, and IS/IT (Scott 2004; Currie 2009). In particular, neo-institutional theory has been applied in several IS studies (Mignerat & Rivard 2009).

Furthermore, it is argued that IS studies have not exploited neo-institutional theory in a level of analysis that goes beyond the organizational level; for instance, to include environmental (e.g., societal, sector, or field) and individual (e.g., agency) issues (Currie 2009).

3.2. Neo-institutional Theory in IS Research

In researching IS/IT-related phenomena, there has been a call to pay attention to institutional influences on the adoption of IS/IT innovations (Swanson 1994). In IS literature, a focus on the use of neo-institutional theory was suggested in order to gain an *"understanding for how technologies are embedded in complex interdependent social, economic, and political networks, and how they are consequently shaped by such broader institutional influences."* (Orlikowski & Barley 2001, p.154). The literature reported that neo-institutional theory was used for *"understanding the impact of internal and external influences on organizations that are engaged in […] IT-induced change"* (Weerakkody et al. 2009, p.355). External influences can be competitors, industry, government agencies, the public, or investors. Internal influences can be perceived benefits, readiness, and sensitivity to cost (Tung & Rieck 2005). Consultancies can also act as a further influence, contributing before, during, and after the adoption of IT innovations (Swanson 2010). Furthermore, many studies have used neo-institutional theory to *"examine IS/IT-related phenomena exemplified in IT innovation, IS development and implementation, and IT adoption and use"* (Mignerat & Rivard 2009, p.1). In the existing literature, the use of neo-institutional theory in IS research has focused on three core themes: the effect of institutional pressures on IS/IT innovation process, the institutionalization process of IS/IT innovations, and the interaction between IS/IT and institutions (Mignerat & Rivard 2009).

One study in particular has used neo-institutional theory to examine the relationship between IS/IT development and implementation, and organizational change (Avgerou 2000). Through an analysis of the history of IS/IT development in a Mexican company, the study suggested that IS/IT innovation is a process of technical-rational and social forces that intensify organizational change rather than drive it.

In the area of IS/IT innovations, one study has identified institutions that influence IS/IT innovations through institutional interventions. In particular, it has examined the influence of government policy on IS/IT innovations (King et al. 1994). In addition to explaining IS/IT phenomena, neo-institutional theory has been used to predict an

organization's intention to adopt IS/IT innovations (Toe et al. 2003). Another study has relied on neo-institutional theory to argue that an organization's internal circumstances, together with the organizing vision of the surrounding community, can shape the likelihood of an organization to innovate with IS/IT (Swanson & Ramiller 2004). Accordingly, the authors introduced four processes for organizational innovation with IS/IT: comprehension, adoption, implementation, and assimilation.

Neo-institutional theory has also been used to understand whether the adoption and diffusion of IS/IT innovation in the healthcare sector will continue or decline; this is influenced by the conflict between the interpretations of IT-induced change from such innovation among institutional groups (Currie & Guah 2007). A further study has examined the effect of regulative and normative influences on the adoption of Western-based electronic human resource management (e-HRM) in Chinese subsidiaries of multinational corporations (Heikkilä 2013). The study found that these influences had positive and negative consequences for subsidiaries. Additionally, the response of subsidiaries to these influences is not likely to allow strategic value to be gained from e-HRM. Regarding IS/IT implementation, one study has examined the influence of coercive and normative pressures on ERP implementation in a Dutch organization, causing the organization to follow an acquiescence strategy as a response to these pressures (Benders et al. 2006).

A study related to the assimilation stage of IS/IT has used neo-institutional theory to explain how the top management championship, strategic investment rationale, and the extent of coordination all shape the assimilation of web technologies within an organization (Chatterjee et al. 2002). Another study has relied on neo-institutional theory to explain the important role of top management in mediating the influence of external institutional pressures on the assimilation of enterprise systems within organizations (Liang et al. 2007). Their study found that the mimetic pressure had a positive influence on the mediation of top management's belief and participation in the assimilation of enterprise systems' ERP; however, the coercive pressure only influenced the mediation of top management's beliefs. Another study questioned the external and internal factors that influence the assimilation of ERP in large Australian organizations (Pishdad & Haider 2013). The study identified eight factors that successfully influence the social and cultural environment of an organization and, consequently, facilitate the assimilation of ERP within it.

In the area of IS security, one study has taken a different perspective, arguing for the use of neo-institutional theory to *"understand, explain, control, and predict"* IS security issues related to social behavior in organizations (Bjorck 2004, p.1). Furthermore, the author discussed the role of standards and organization's policies in controlling the social behavior related to the securing of IS/IT. In another study, three economic-based factors were identified, and quantitatively proven to moderate the institutional influences on the adoption of IS security innovations (Hsu et al. 2012). Furthermore, three organizational capability factors were shown to moderate the assimilation of IS security innovations.

In the area of IS/IT outsourcing, neo-institutional theory has been used in a wide range of studies (Hirschheim et al. 2007). The literature has reported that Kodak's total and major outsourcing decision acted as a mimetic pressure to positively influence subsequent IS/IT outsourcing adoptions (Lacity et al. 2010; Loh & Venkatraman 1992b). Another study, which had a focus on the banking industry, investigated the strategic responses (e.g., conform to or resist) of individual banks to institutional influences on IS/IT outsourcing (Ang & Cummings 1997). These responses depend on the degree of institutional influences, the economic gains from IS/IT outsourcing, how far it is financially possible to resist institutional influences, and transaction cost factors.

Another study used the concept of organizing vision proposed by (Swanson & Ramiller 1997), to explain how the first wave of ASP providers happened to fall out of the market with the rise of the dot.com bubble and the emergence of web services providers (Currie 2004). A recent study explored factors that increase or reduce organizational responsiveness to anti-offshoring institutional pressures (Khan & Lacity 2014). This study proved that an organization's responsiveness is increased by mimetic pressures and by that organization's expectations of social legitimacy. Furthermore, an organization's responsiveness is reduced by conflicting goals and uncertainties in the legal environment.

The IS literature features a critical discussion of the challenges that face IS researchers in applying neo-institutional theory and the limited scope of using it in IS/IT-related studies (Currie 2009; Mignerat & Rivard 2009; Weerakkody et al. 2009). One of the challenges is the multifaceted nature of the theory (i.e., organizational field, structural isomorphism and institutional logics) and the blurriness of its concepts (i.e., institutions) (Currie 2009). In these studies, the institution was always treated as an

entity or organization, rather than, for instance, a piece of technology or top management support (Mignerat & Rivard 2009; Currie 2009). The unit of analysis in IS/IT studies has always been the adoption of IS/IT innovation within the organization, despite the fact that the IS literature has advocated the need for a broader unit of analysis (e.g., field, industry, sector, society, country, and systems) (Weerakkody et al. 2009; Mignerat & Rivard 2009; Currie 2009), given that institutional forces come from multiple levels, including the environment and organizations (Currie 2009, p.74).

Furthermore, the IS literature has reported on the lack of qualitative and interpretive studies that have used neo-institutional theory in studying IS/IT phenomena (Weerakkody et al. 2009). Additionally, few IS/IT studies have used the five strategic responses to institutional pressures by (Oliver 1991). Even then, the focus has been on acquiescence strategy, despite the fact that IS/IT adoption may involve the other four strategies (Mignerat & Rivard 2009). Furthermore, the concept of institutional logic has rarely been applied in the IS literature. The exception is a study that focused on understanding the conflict between past and present logics and the changes this has brought to the governance systems and work practices in the healthcare sector (Currie & Guah, 2007).

3.3. Neo-institutional Theory and Cloud Computing Adoption

CC is argued to be embedded into political reforms and organizational changes to enact, support, and drive transformation in the way organizations run their business (Cordella & Willcocks 2012). In the CC literature, governmental influence was reported to be negative on the adoption of CC services; however, this only applies for highly regulated industries such as healthcare (Schneider & Sunyaev 2014). At the national level, laws and regulations can be tough, with penalties constraining the adoption of CC services in some contexts (Seddon & Currie 2013), or encouraging, with policies motivating the adoption of CC services in other contexts (Lian et al. 2014).

Furthermore, at the international level, laws and regulations give rise to complexity and fuzziness issues (Marston et al. 2011); for instance, in the EU region there is serious concern about data security and privacy issues with regard to public records. Indeed, the unsolved conflicts in legislation between the EU and US. This raises a big question mark regarding responsibilities and accountabilities between client organizations and CSPs (Seddon & Currie 2013), especially with widespread leaks

about the NSA PRISM surveillance program, which has led to increased uncertainty (Schneider & Sunyaev 2014; NTT Communications 2014).

In the context of CC, the organizational field that is most characterized by high competition, uncertainty, and conflicts consists of various actors such as "national governments, supra-national organizations, industry bodies, trade and professional associations as well as cloud vendors, cloud clients and the organizations of these clients" (Kshetri 2013, p.375). These actors enact the rules and norms of the CC game through an exchange of dialogues, rhetorics, and content; however; these rules and norms are not moving at the same speed as the technological development (Kshetri 2013). This has been attributed to the fact that each of these actors has a different logic and perception of the main CC issues, namely, concerns, interests, and capabilities (Kshetri 2013). Some actors are focused on costs benefits, some are focused on security and privacy risks, whilst some are focused on security and privacy risks, and others are focused on controlling the data in the cloud, either by securing or spying on data (Kshetri 2013).

Furthermore, the literature has encouraged focusing research efforts on investigating *"factors other than technology characteristics, such as organizational, individual, and environmental characteristics…. [and] further investigation of institutional influences in the context of cloud-sourcing decisions"* (Schneider & Sunyaev 2014, p.15).

A limited amount of empirical research has sought to apply concepts from neo-institutional theory in order to examine the effect of institutional influences on the adoption of CC services. Three studies are in progress, which have chosen to use a neo-institutional perspective. One of these studies is aimed at understanding the behavior of cloud vendors in how they formulate their strategies to respond to the emerging market of CC (Su 2011). The second study has focused on the clients by arguing that institutional influences are likely to affect a client organization's perception of CC characteristics (e.g., accessibility, scalability, cost-effectiveness, and lack of security); in turn, this has an influence on its ultimate intention to adopt CC services (Saya et al. 2010). The third study hypothesized that the successful adoption of SaaS by peer organizations serves as a mimetic pressure to influence the likelihood of a client's decision to adopt SaaS (Xin & Levina 2008).

Only one empirical study found that, in quantitative terms, the mimetic pressure (e.g., the perception that competitors have adopted CC services successfully) has a significant influence on the intention of client organizations to adopt CC services in

Germany (Messerschmidt & Hinz 2013). Nonetheless, the quantitative methodological stance is predominant, with all three of these studies in progress planning to conduct surveys.

The way in which client organizations interpret these various influences in their adoption strategies and their reasons for so doing remain relatively unexplored. Thus, I used the concept of isomorphic pressures (DiMaggio & Powell 1983) and strategic responses to these isomorphic pressures (Oliver 1991). I, then, applied these concepts to the findings from two case qualitative studies: one from Egypt and one from Norway. According to the IS literature: *"organizations in different socio-economic and political contexts may often react differently to similar internal and external challenges due to constraints imposed by the environment they exist in"* (Weerakkody et al. 2009, p.354). Thus, my objective was to explore more institutional influences in those two different contexts and examine the way in which client organizations interpret such influences in their adoption strategies. The institution that I focused on in my research is the "adoption of CC".

In constructing the analytical framework in Paper1, the concepts of neo-institutional theory were placed into the context of CC adoption. In this conceptual paper, the aim was to be more descriptive than normative in examining the plausibility of the framework by bringing in relevant literature on the use of CC in enterprise systems. It is important to understand how an organization interprets changes at the field level. However, it is equally important to gain insights into why an organization decides to adopt a certain strategic response over others. Both external and internal factors may be considered in this process. Field-level changes involved in the enactment of new government regulations, the ways in which business partners collaborate, and the advent of new CC services can all trigger various isomorphic pressures. The relevant organizations at the field level are summarized in Table 4, whilst the types of isomorphic pressures that influence the adoption of CC are presented in Table 5. Table 6 presents the strategic responses that resulted from the client organization's interpretation of the isomorphic pressures.

Table 4: Organizations at the field level (Paper1)

Organization	Description	References
CSPs	Various forms of CC (SaaS, PaaS, and IaaS) offered by CSPs, along with their promised benefits and associated potential risks, affect CC adoption.	(Armbrust et al. 2010)

Organization	Description	References
Peer organizations	Organizations develop this trust through asking their peers about their perceptions of CSPs' capabilities and reputations.	(Altaf & Schuff 2010) (Heart 2010) (Yao et al. 2010)
Business partners	Business partners (e.g., customers and suppliers) may affect the organization's decision to adopt CC services in order to keep on their partnership.	(Li et al. 2012)
Professional and industry associations	Professional and industry associations may develop guidelines to facilitate CC adoption, as well as evaluation criteria to select appropriate CSPs.	(Badger et al. 2011) (Kshetri 2012)
Regulators	Regulators may enact obligations on CSPs to inform the adopting organizations about the protection of data security, privacy, and integrity. This is more important among government agencies.	(Marston et al. 2011) (Kshetri 2012)

Table 5: Isomorphic pressures (Paper1)

Isomorphism	Description	References
Coercive	Organizations adopt CC for regulatory compliance reasons or because they forced by other organizations through compulsory power.	(Chong & Ooi 2008) (Low et al. 2011) (Herhalt & Cochrane 2012) (Zielinski 2009) (Li et al. 2012)
Normative	Organizations adopt CC because they are influenced by learning processes or a convincing power of other organizations.	(Low et al. 2011) (Herhalt & Cochrane 2012) (Yao et al. 2010)
Mimetic	Organizations adopt CC to become similar to other adopting organizations, without a thorough reflection process.	(Benders et al. 2006) (Parakala & Udhas 2011) (Sultan 2011)

Table 6: Strategic responses (Paper1)

Strategy	Example of response	References
Acquiescence	Organizations adopt CC with or without any reflection. Some of them conduct a proper study and decide to choose full	(Chong & Ooi 2008) (Herhalt & Cochrane 2012)

Strategy	Example of response	References
	implementation, while others do so simply by following the norms, business hype, and/or regulatory force.	
Compromise	Organizations develop an adoption strategy, such as by adopting CC to run parts of their strategic information systems or by combining public and private/community clouds.	(Parakala & Udhas 2011) (Herhalt & Cochrane 2012)
Avoidance	Organizations adopt partial implementation and conduct testing of a proof of concept, such as using CC to run parts of their nonstrategic information systems.	(Herhalt & Cochrane 2012) (Lin & N. Chen 2012)
Defiance	Organizations decide not to adopt CC at all.	(Herhalt & Cochrane 2012) (Ernst&Young 2012) (Yao et al. 2010)
Manipulation	Organizations establish their own private or community CC.	(Herhalt & Cochrane 2012) (Marston et al. 2011) (Parakala & Udhas 2011) (Brian et al. 2012)

I wrote Paper1 based on a review of the literature and by identifying a research gap; although it was written before I began to collect data, the theory did not guide my data collection. I chose to freely explore the factors that influence the adoption of CC services by, first, conducting an exploratory Delphi study. The Delphi study guided my selection of the two qualitative case studies from Egypt and Norway. In the next chapter, I offer an explanation of my research approach.

3.4. Summary of the Chapter

In this chapter, I have argued for my theoretical choices and introduced the concepts borrowed from neo-institutional theory (i.e., isomorphic pressures, strategic responses, and institutional logics) to guide my data analysis. I reviewed the use of neo-institutional theory in IS research, including IS/IT outsourcing, and in CC in particular. I highlighted the gap in using neo-institutional theory to study the CC phenomenon. In my first paper (cf. Paper1), I defined the organizational field, isomorphic pressures, and strategic responses in the context of CC in accordance with the literature. In the next chapter, I go on to discuss the research approach I took to answer the research questions.

“If we knew what it was we were doing, it would not be called research, would it?”

― Albert Einstein

4 Research Approach

This thesis addresses three research questions (one main RQ and two SQs), which I introduced in Chapter 1. In addition, it focuses on understanding the phenomenon of CC adoption and how it is influenced by internal and external factors. In Chapter 2, the existing body of IS research is reviewed and the research gaps are highlighted and discussed. In this chapter, I begin by giving an overview of my research design that includes interpretive research approach, research methods, theory, research questions, and research publications. In Section 4.1, I argue for my philosophical and methodological choices. In Section 4.2, I provide an overview of my research activities in terms of publication, data collection, and data analysis timelines. In Section 4.3, I provide details about my sampling strategy and demographics about the informants. In Section 4.4, I report on my research settings, data collection and analysis. Finally, in Section 4.5, I offer some reflections on validity issues related to my research approach.

4.1. Research Design

As presented in Chapter 2, the CC adoption phenomenon and the factors that influence it are the result of social interaction between organizations, which is reflected in the opinions of their staff from going through a particular experience. Thus, the knowledge gained about the phenomenon of CC adoption is socially constructed. Hence, this is in line with the ontological assumption of the interpretivist approach. Interpretivism perceives organizations as social processes in which the world is interpreted in a particular way in order to legitimatize shared actions and establish shared norms (Checkland & Holwell 1999). Ontologically speaking, in relation to CC adoption, decisions are made to use CC services and are used by people (within client organizations), offered by people (within CSPs and consultancies), and governed by people (within governments). Thus, CC is related to people in particular and social settings (organizations) in general. As circumstances change over time, interactions between these social systems change, and so do the interpretations of reality about what influences the adoption of CC (Orlikowski & Baroudi 1991; Kshetri 2013).

In epistemological terms, since CC adoption is a social process, I chose to acquire knowledge about it from the interpretations of the stakeholders involved (i.e., clients, providers, consultancies, and academics). I regard these stakeholders as constituents of the practices and norms of CC adoption. This aligns with the epistemological assumptions of the interpretive approach, namely that, *"the language humans use to*

describe social practices constitutes those practices. Thus, understanding social reality requires understanding how practices and meanings are formed and informed by the language and tacit norms shared by humans working towards some shared goal." (Orlikowski & Baroudi 1991, p.14).

In the subsequent sections, I report on my research methodology, because *"interpretive researchers are not saying to the reader that they are reporting facts; instead, they are reporting their interpretations of other people's interpretations. It is thus vital, in order to establish some credibility to the reader, that they describe in some detail how they have arrived at their 'results'."* (Walsham 1995, pp.78–79). This includes details on the chosen research methods and the reasons for making these choices, the number of informants interviewed and their demographics, research context and reasons for choosing this context, other data collection sources, unit of analysis, and the analysis techniques (Walsham 1995). Thus, the reader can track the procedures used to reach my findings (Miles & Huberman 1984a).

I approached the study on CC adoption by, first, conducting a systematic literature review to gain wider knowledge about previous research that has contributed to our understanding of CC adoption. In so doing, I followed the guidelines put forward by (Webster & Watson 2002; Okoli & Schabram 2010; vom Brocke et al. 2009). Consequently, I was able to identify any empirical, theoretical, or methodological gaps (Paper2). Hence, Paper2 helped to formulate the two SQs. It should be noted that I began this systematic literature review at a very early stage of my PhD, before working on and writing Paper1. Paper1 is based on a selective literature review relating to neo-institutional theory and CC literature; thus, it provided a theoretical foundation for answering the main RQ. This involved defining the organizational field in the context of CC adoption, and constructing a framework to guide the analysis of the empirical data. Second, I conducted a ranking-type Delphi study (Schmidt 1997) to generate a list of the most important CC adoption issues identified and prioritized by CC experts (Paper5). The Delphi procedure is "a rapid and efficient way to cream the tops of the heads of a group of knowledgeable people" (Dalkey 1972, p.16). Furthermore, the ranking-type Delphi survey is argued to be a rigorous data collection method. In particular, it can be used to produce a rank-ordered list of subject matters (Schmidt et al. 2001). Additionally, the Delphi method is well-suited to build consensus on a topic that is spread across various disciplines (Hsu & Sandford 2007), such as CC. The Delphi study involved three phases (i.e., brainstorming, narrowing

down, and two rounds of ranking) (Okoli & Pawlowski 2004) in addition to follow-up interviews.

The outcomes of the Delphi study address the main RQ and two SQs. I provide details on the Delphi procedure in Section 4.4.1; however, during the first phase of the Delphi study and the follow-up interviews, I had some interesting inputs from the experts, themselves. These experts came from Egypt and Norway, and were able to provide interesting answers relating to the context of each country, particularly, its ICT and legal infrastructures. This guided my choice of the case studies and provided inputs to them. Consequently, two qualitative exploratory case studies were chosen; one from a developing country (Egypt) and one from a developed country (Norway). The reasons for having two case studies are to gain more knowledge about the factors that influence the adoption of CC in relation to both contexts. Furthermore, the Egypt case was convenient for me, because Arabic is my mother tongue and it was easy to communicate with the Egyptian informants. For the Norway case, some Norwegian informants were able to express their opinions and experience in English, so I was able to communicate with them. However, others preferred to use the Norwegian language during the interview and to answer the Delphi's brain storming questionnaire. This was a major challenge for me, because I was unable to acquire the Norwegian language skills in time. I have overcome this problem with the assistance of my supervisors, who translated the informants' answers to the brainstorming questionnaire, facilitated the Norwegian interviews, and translated their transcriptions.

Third, limited empirical research was carried out into CC adoption in the Egyptian and Norwegian contexts, which was reported in Paper3 and Paper4. Consequently, two exploratory case studies were conducted (Yin 2009; Marshall & Rossman 1989). Case study method is useful for exploring areas where existing knowledge is limited (Cavaye 1996). Thus, case study strategy aims to provide a description of the phenomenon by understanding the dynamics of its context (Darke et al. 1998; Eisenhardt 1989; Yin 2009). Furthermore, case study strategy in IS research helps to understand and interpret the human/technology interaction in the natural social setting (Orlikowski & Baroudi 1991). The findings from the two case studies were analyzed using neo-institutional theory concepts introduced in Paper1. Figure 4 depicts the research design I followed to answer the research questions, along with the theory and methods used in the published papers.

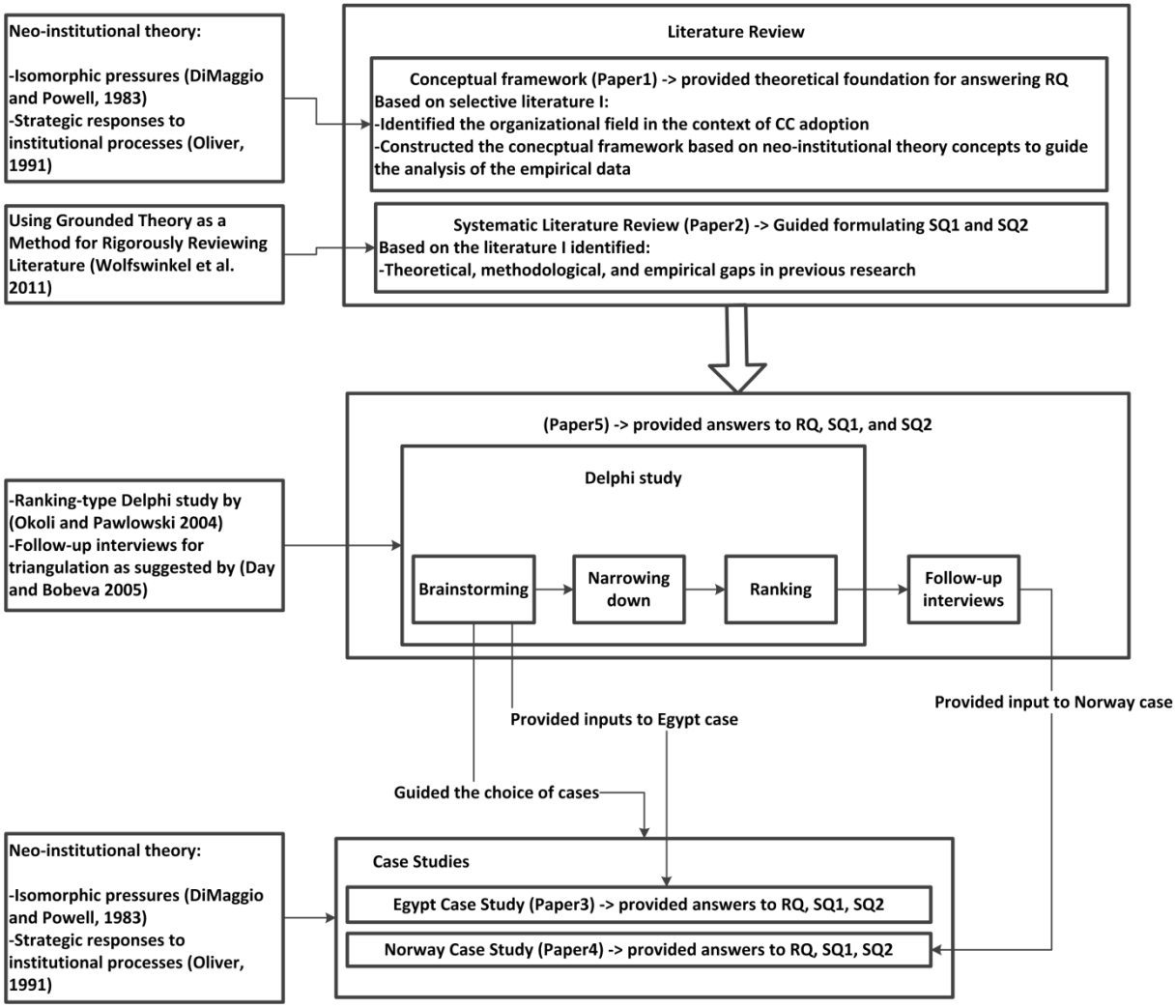


Figure 4: Research design

4.2. Research Activities

Work on this PhD thesis took three years, during which time I carried out a set of activities, including a literature review and empirical studies that involved data collection and analysis. The publications that resulted from these studies will be presented later in this thesis. As illustrated in Figure 5, the Delphi study is the first study I started and the two case studies took place in parallel with it. Papers1 and 2 are based on the literature, through which problem formulation took place. Papers3 and 4 are based on each of the case studies. Paper5 is based on the Delphi study. Figure 5 also demonstrates the data collection and analysis activities for the empirical studies.

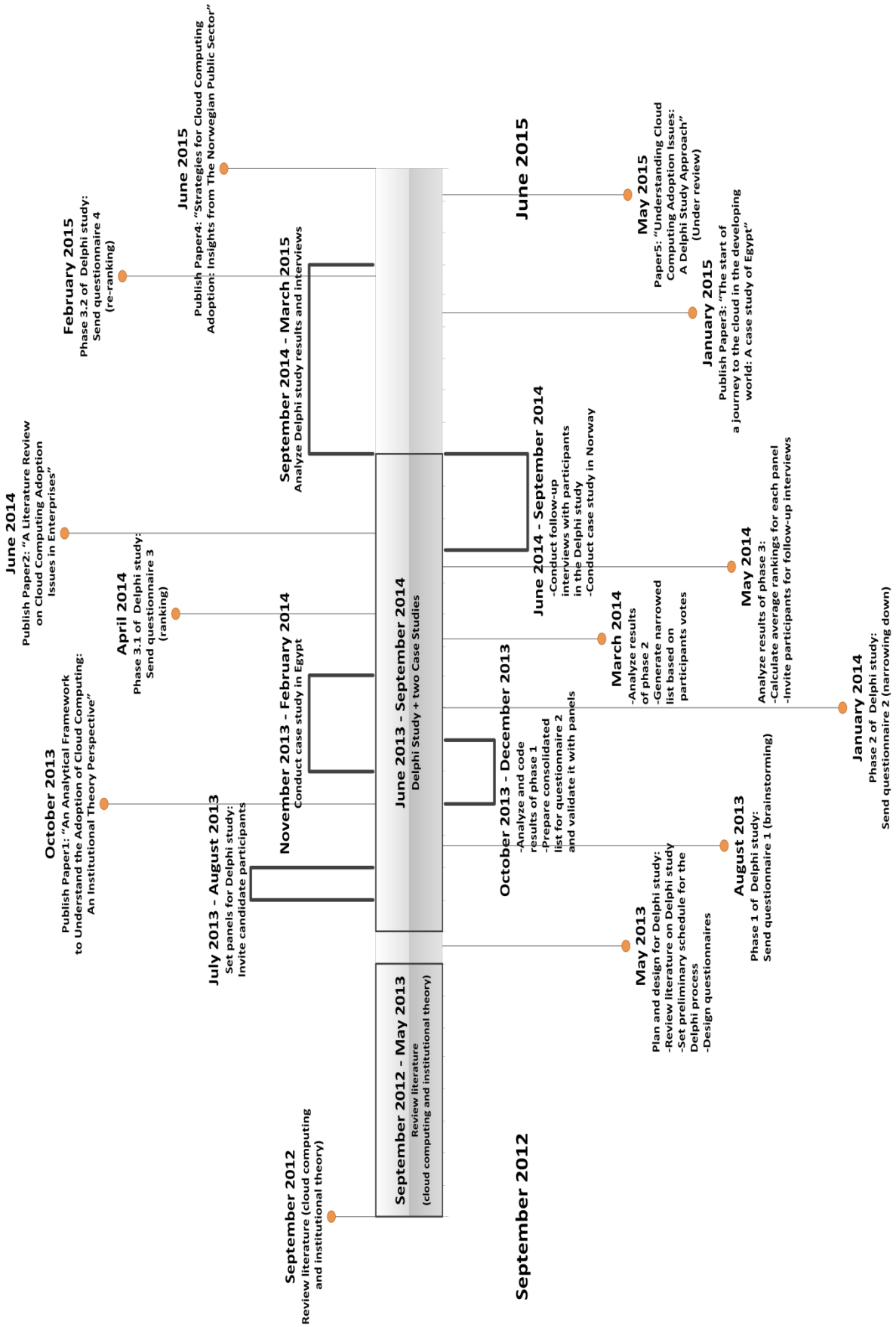


Figure 5: Overview of research activities

4.3. Getting Informants Onboard

The Delphi study was the first empirical study carried out; thus, my planning involved searching for informants that come within the scope of the study. Thus, the purposive sampling strategy was seen to be appropriate (Day & Bobeva 2005). Although other studies may have used the term "participants", I prefer to use the term "informants" instead. According to Bygstad and Munkvold (2010), an informant is defined as a stakeholder that gives qualified information or opinion on a case. This definition applies to the nature of my study and the involvement of the informants in my study, as my informants were stakeholders from different domain backgrounds who gave their opinions throughout the study even during the Delphi questionnaires. Thus, the aim was to gain the informants' opinions and interpretations rather than their sufficient sample representativeness. Searching for informants to participate in the Delphi study involved surveying literature sources such as academic papers, practitioners' articles, professional business networking sites (e.g., LinkedIn), and reference contacts in order to target the candidate informants with considerable IT expertise in the field and who are currently involved in CC adoption initiatives. My supervisors also assisted in making contact with some informants. The number of years of IT expertise was the main criterion for regarding an informant as an expert. For this study, an expert needed to have a minimum of three years of IT expertise. They also had to be involved in the CC adoption area. The experts who participated in the Delphi study had IT experience ranging from five years to 30 years. Invitations were initially sent to 60 experts of whom 34 agreed to participate in the study. After the 34 experts had agreed to participate, a scheduled plan was sent to them.

This resulted in three heterogeneous groups of experts (i.e., service providers, clients, and academics) who found the study relevant to them. The involvement of practitioner and academic experts is helpful in gaining a better understanding of various issues related to the phenomenon under study (Ward 2012). Furthermore, the experts were from different sectors, industries, and countries, thus representing diverse opinions and experiences on CC adoption issues. Academic experts showed interest as they were involved in field studies relating to CC adoption. Clients showed interest, because they were early, late, or potential adopters and were willing to share their experiences and concerns about CC. Providers showed a willingness share their views on CC issues from the perspective of IT vendors, CSPs, cloud service brokers, and IT consultancy organizations.

I agreed to give the experts a report of the final results of the study, which helped to motivate their interest in participating in the study (the report of final results is provided at the end of Appendix B). E-mail communication with experts took place during the completion of the Delphi surveys for convenience. Table 7 provides a detailed profile of the experts, their codes (i.e., codes are C for clients, P for providers and consultants, and A for academics along with ordered numbers for each group of informants), and an indication of the contribution of each informant to the Delphi study (DS), Egypt case study (ECS), and Norway case study (NCS).

In the Delphi study, clients C1 and C6 are from the same organization; they work in the Pakistan subsidiary of a worldwide organization. Client C13 worked for a client organization at the beginning of the Delphi study; however, by the third questionnaire, he had changed job and worked for a worldwide IT vendor and CSP. This implies that his background is a mix of client and CSP experiences. Clients C2 and C3 are from same client organization; C3 was not part of the Delphi study, but was invited by C2 to join the follow-up interview, because of his technical knowledge of the CC project being implemented. Furthermore, five academics agreed to be informants for the Delphi study. Although the sample is relatively small, it provided rich inputs based on previous research carried out in the area of CC or other relevant areas such as IT innovation, enterprise systems, and services innovation. I met two of the academics, A3 and A2, at a workshop on CC for development. Academic A1 was a guest lecturer on one of the PhD courses that I attended; his research interest is in enterprise systems and service innovation. Academic A5 was invited based on the suggestion of another academic whom I invited first, but was too busy to take part. Academic A4 was invited through my supervisors as they knew a priori that his area of interest is CC.

Some Norwegian informants took part in the Delphi study and were also able to give an insight into my choice of Norway as a case study and provided an input into that study. I decided that their number and input meant that I did not need to invite more Norwegian informants, because this would have led to saturation (Eisenhardt 1989). In addition, two Egyptian informants took part in the Delphi study. I was put in touch with provider P14 through a contact of a colleague; this contact suggested that I should interview P14. The interview with P14 was to explore the Egyptian context. As a result of the interview, I invited him to join the Delphi study. The interview had to be made in person, because he works for a government-established CSP. At this meeting, I described my research focus and explained my plan to set up a Delphi panel. The informant showed an interest in joining the Delphi study. During the interview, he

talked about a government initiative known as “Cairo ICT” and the Egyptian CC strategy. This gave me an interest insight into my choice of Egypt as a case study. Thus, P14 contributed to the Delphi study and his discussion guided my choice of Egypt as a case. Informant C13 was interviewed as part of the Delphi study’s follow-up interviews; he provided insights into the cultural issues related to the Egyptian context, particularly in terms of the difficulty to convince clients about the benefits of CC.

However, I still needed to recruit more Egyptian informants for the case study. Thus, I invited 11 informants, all of whom I reached through the LinkedIn Professional Networking website or through the suggestions of my colleagues. I followed the same sampling strategy in choosing the additional Egyptian informants. My choices were based on their knowledge about and/or experience of CC (Palinkas et al. 2013; Patton 1990). I should point out that none of my colleagues were included in my sample; they only served to put me in contact with the relevant informants. Informants C14 and C15 are from same client organization and they work at the data center of an organization. Likewise, informants P22 and P23 are from the same worldwide IT vendor and CSP. I was already following posts from informant P26 on Facebook through a community for MS SharePoint; thus, I invited him for an interview. I reached informant P18 through a colleague who works in the same worldwide IT consultancy, an integrated communications provider, and CSP. The colleague forwarded my request to a contact in another department who then put me in touch with P18, as he is responsible for CC solutions.

There are limitations regarding my informants that I would like to elaborate on here. I was not successful in recruiting as many clients in my sample for the case study of Egypt as in the case study of Norway. In particular, in my sample for the case study of Egypt, CSPs and consultancies dominated. Despite this limitation, they were able to offer insights about the client organizations they dealt with. With regard to the Norway case, I had six informants from five client organizations in the public sector (three different municipalities and two different government authorities). For the Delphi study, 34 informants were from six countries, 13 industries of varying company types (public and private), company sizes (large, SME, and micro), and five degrees of job roles. However, I did not have the same number of informants from each country, industry, sector, or size. Norwegian informants dominated the Delphi study sample.

Table 7: Informants' profile

#	Code	Position	Found through	Company type	Company size	Sector	Country	Contribution		
								DS	ECS	NCS
1	P1	Vice president and general manager cloud services	LinkedIn	Worldwide cloud service broker	SME	Private	USA	X		
2	P2	Director cloud service	LinkedIn	Worldwide IT vendor and CSP	Large	Private	Norway	X		
3	P3	CEO	My supervisors	National CSP	Micro	Private	Norway	X		
4	P4	Regional Offer Director for Cloud Transformation	My supervisors	Worldwide IT vendor and consultancy	Large	Private	Norway	X		
5	P5	CEO	LinkedIn	National IT consultancy	Micro	Private	UK	X		
6	P6	CEO	My supervisors	Worldwide IT vendor and CSP	SME	Private	Norway	X		
7	P7	Product and R&D Manager	My supervisors	Worldwide IT vendor	SME	Private	Norway	X		
8	P8	Software Engineer	My supervisors	Worldwide IT consultancy	Large	Private	Norway	X		
9	P9	Owner and senior consultant	My supervisors	National IT vendor and consultancy	SME	Private	Norway	X		
10	P10	CTO	My supervisors	Worldwide IT consultancy	Large	Private	Norway	X		
11	P11	SVP and CMO	LinkedIn	Worldwide IT vendor (wireless technologies)	SME	Private	USA	X		
12	P12	Senior Consultant, team leader CRM, and Cloud Advisor	My supervisors	Worldwide IT consultancy	Large	Private	Norway	X		X
13	P13	Product Manager	LinkedIn	Worldwide IT vendor and CSP	SME	Private	Norway	X		X
14	P14	Technical Operation Manager	A colleague -> reference	National CSP and IT consultancy (government agency)	SME	Public	Egypt	X	X	
15	P15	Business Development Manager	My supervisors	Worldwide IT vendor, CSP, and IT consultancy	Large	Private	Finland	X		

#	Code	Position	Found through	Company type	Company size	Sector	Country	Contribution		
								DS	ECS	NCS
				(Telecommunications)						
16	P16	Senior consultant	My supervisors	Scandinavian IT consultancy	Large	Private	Norway	X		X
17	P17	Senior consultant	My supervisors	Scandinavian IT consultancy	Large	Private	Norway	X		
18	C1	Director – global IT services	LinkedIn	Client organization (Worldwide telecommunications)	Large	Private	Pakistan	X		
19	C2	Vice president	My supervisors	Client organization (Government administration agency)	Large	Public	Norway	X		X
20	C3	Technical project manager	LS	Client organization (Government administration agency)	Large	Public	Norway	X		X
21	C4	Enterprise architect	My supervisors	Client organization (Government Healthcare agency)	Large	Public	Norway	X		X
22	C5	CIO	My supervisors	Client organization (Public municipality)	Large	Public	Norway	X		X
23	C6	IT service delivery manager	LinkedIn	Client organization (Worldwide telecommunications)	Large	Private	Pakistan	X		
24	C7	IT manager	LinkedIn	Client organization (Public municipality)	Large	Public	Norway	X		
25	C8	Director information services	My supervisors	Client organization (Worldwide oil and gas)	Large	Private	Norway	X		
26	C9	CIO	My supervisors	Client organization (Public municipality)	SME	Public	Norway	X		X
27	C10	Senior IT advisor – business processes	My supervisors	Client organization (National power supplier)	Large	Private	Norway	X		
28	C11	IT advisor	My supervisors	Client organization (Public municipality)	Large	Public	Norway	X		X
29	C12	CIO	LinkedIn	Client organization	Large	Private	Norway	X		

#	Code	Position	Found through	Company type	Company size	Sector	Country	Contribution		
								DS	ECS	NCS
				(Worldwide chemicals)						
30	C13	Cloud infrastructure administrator	LinkedIn	Client organization (Worldwide telecommunications)	Large	Private	Egypt	X	X	
31	P18	Senior solution manager	A colleague -> reference	Worldwide IT consultancy, integrated communications provider, and CSP	Large	Private	Egypt		X	
32	P19	Co-founder and manager	LinkedIn	CSP, a partner of worldwide CSP in Egypt	SME	Private	Egypt		X	
33	P20	Software development engineer	LinkedIn	Worldwide CSP	Large	Private	Egypt		X	
34	P21	Senior IT consultant	LinkedIn	National IT consultancy	Micro	Private	Egypt		X	
35	P22	Managing IT consultant	LinkedIn	Worldwide IT vendor and CSP	Large	Private	Egypt		X	
36	P23	Account manager	LinkedIn	Worldwide IT vendor and CSP	Large	Private	Egypt		X	
37	P24	Consulting system engineer	LinkedIn	National IT consultancy	Micro	Private	Egypt		X	
38	P25	IT consultant	LinkedIn	National IT consultancy	Micro	Private	Egypt		X	
39	C14	System engineer	A colleague -> reference	Client organization (Higher education)	-	Private	Egypt		X	
40	C15	System engineer	A colleague -> reference	Client organization (Higher education)	-	Private	Egypt		X	
41	P26	Technical consultant	Facebook community for MS SharePoint	National CSP	SME	Private	Egypt		X	
42	A1	Professor	Course	University	-	Public	Norway	X		
43	A2	Research Fellow	Workshop	University	-	Public	Norway	X		
44	A3	Associate Professor	workshop	University	-	Public	Norway	X		
45	A4	Senior Lecturer and Consultant	My supervisors	University	-	Private	Norway	X		
46	A5	Researcher	Reference	Research institute	-	Private	Norway	X		

4.4. Data Collection and Analysis

My data collection approach involved conducting three Delphi surveys and interviews. With regard to data collection, the interpretive approach views such activities in the following light: *"What we call our data are really our own constructions of other people's constructions of what they and their compatriots are up to"* (Geertz 1973, p.9). Further details about the data collection procedures used in my work are provided in the sub-sections that follow. In addition, I gathered secondary data sources, including official documents, online news articles, presentation slides, reports, video recordings, and literature. These secondary data sources help to avoid researcher's bias by providing multiple measures of the same phenomenon and by triangulating data collected from informants to avoid conflict of information (Miles & Huberman 1984b; Darke et al. 1998). However, it is natural that the interpretive researchers are driven by subjectivity in their analysis of data; such subjectivity is driven by their beliefs, values, and interests, and shapes the investigation (Orlikowski & Baroudi 1991). This is applicable to the analysis of the data for the two case studies and the follow-up interviews of the Delphi study.

However, when analyzing the data from the last two phases of the Delphi surveys, I applied statistical analysis methods, using IBM SPSS Statistics tool to eliminate subjectivity. Furthermore, the consolidated list of issues that resulted from the first Delphi survey was validated by the participants. The pluralism in using quantitative and qualitative methods is desirable in IS research, serving as a means of triangulation to examine different dimensions of the same research problem (Mingers 2001; Jick 1979). Triangulation means "the combination of methodologies in the study of the same phenomenon" (Denzin 1978, p.291); it provides a wider range of knowledge on which research can be based (Mingers 2001). Furthermore, "between-method" triangulation insures the degree of external validity and improves the accuracy of judgments by collecting different kinds of data bearing on the same phenomenon (Jick 1979).

In sub-section 4.4.1, I explain in detail the data collection and analysis details that took place during the three Delphi surveys. In sub-section 4.4.3, I provide details on the interviews that have been conducted to follow-up on the Delphi study, and to collect and analyze data for the two case studies. This includes duration, mode of communication, and date of each interview. In sub-section 4.4.4, I list the secondary data sources, along with the purpose of using each source.

4.4.1. Ranking-type Delphi Study

The aim of this Delphi study is to identify and rank the most important issues of concern in the area of CC adoption. This is achieved by gaining consensus on these issues among the different stakeholders. These issues are important for practitioners to consider in their decisions about CC adoption. Thus, the Delphi method is appropriate for *"identifying and prioritizing issues for managerial decision-making"* (Okoli & Pawlowski 2004, p.1).

Furthermore, by identifying current important issues, IS scholars' efforts to dig into these issues can be better directed. The literature advocated the need to focus on one particular issue: *"what are the obstacles to cloud adoption, rank-ordered by concern, cost, and impact?"* (Andriole 2012, p.68). Thus, a "ranking-type" Delphi study was conducted (Schmidt 1997).

The study was carried out in close collaboration with my supervisors, who gave guidance throughout the design, data collection, and analysis of the study's results. The study was designed using the principles and guidelines documented in the Delphi literature in order to ensure the validity and creditability of the study (Franklin and Hart, 2007, Okoli and Pawlowski, 2004, Day and Bobeva, 2005).

Communication with experts took place remotely through e-mails for convenience. The study involved a set of sequential rounds (i.e., brainstorming, narrowing down, and two rounds of ranking (Okoli & Pawlowski 2004)). The first round was followed by a feedback round to validate the consolidated list of CC adoption issues.

In addition to the Delphi surveys, we conducted follow-up interviews with 16 of the experts participating in the Delphi study. The purpose of the interviews was to enrich and contextualize the existing data in order that stronger conclusions could be drawn during triangulation (Day & Bobeva 2005).

The Delphi surveys and results were e-mailed separately to each expert in order to guarantee full anonymity and thus reduce the effect of dominant individuals (Dalkey 1972). In addition, statistical analysis was employed to reduce the group pressure for conformity and ensure that each expert's answer is well-represented in the final round (Dalkey 1972). Thus, we were able to avoid both researcher bias and informant bias. Table 8 summarizes the design choices made for the Delphi study.

Table 8: Delphi study design

Criteria	Choice
Purpose of the study	Exploration of concerning issues that enterprises are confronted with when adopting CC services and rank these issues
Number of rounds	4 + follow-up interviews with some of the experts
Experts	Heterogeneous divided into 3 subpanels (provider, client, and academic)
Mode of operation	Remote access
Anonymity of the panel	Full
Communication media	Computerized (i.e., e-mail)
Concurrency of rounds	Sequential set of rounds (brainstorming, narrowing down, and two ranking)

Figure 6 summarizes the Delphi study process and the follow-up interviews. In the brainstorming phase, an open-ended question was sent to each expert via e-mail to solicit his/her knowledge about CC adoption issues: "What are the issues that enterprises are confronted with when adopting cloud computing services?". This question was attached to a MS Word file along with a description of the study and instructions for answering the question. Each expert was asked to provide at least six issues related to answering our question (See Appendix B for the structure of this questionnaire). Furthermore, each expert was asked to specify the issues, to justify their importance and consequences, and, if possible, make additional comments to elaborate on the issues concerned.

The experts were given one week to answer the first questionnaire. Some experts responded within one week; however, we had to send several weekly reminders before we received responses from the remaining experts. Eventually, we received answers from 34 experts. Alongside their answers were interesting feedback and comments; for example, client C4 was willing to offer additional clarifications: *"Please see attached questionnaire. Contact me if you have questions and good luck with your work."* Similarly, client C10 also gave a note about the answers she provided: *"I've tried to fill out the questionnaire – it's important to say that this is from the perspective as a system administrator/business process owner. I know it's only briefly described, but please let me know if I should elaborate more specific comments."*

Client C12 also gave a very interesting comment: *"Cloud technology will become a game changer however, it is a young phenomenon, and it is suffering from teething*

pains typical of its age. It's also subject to many overblown hype in the marketplace. Although the upside of cloud computing is big, numerous challenges lie ahead."

In addition, academic A3 provided some particularly interesting feedback: *"Note that the term adoption refers to the process from the enterprise first decides to adopt cloud service to the implementation and becoming a routinized practice. Does this mean that you do not include the process before it is decided to adopt - i.e. searching for solutions and deciding why and how to use cloud? If so, you could be a bit clearer. Another related issue is that (as I write in my attached answer) companies may choose very well cloud services without any central decision, if a decision at all. This is also the nature of cloud (plug-and-play, cheap (sometimes for free)). You may want to take that into consideration and keep up the good work."*

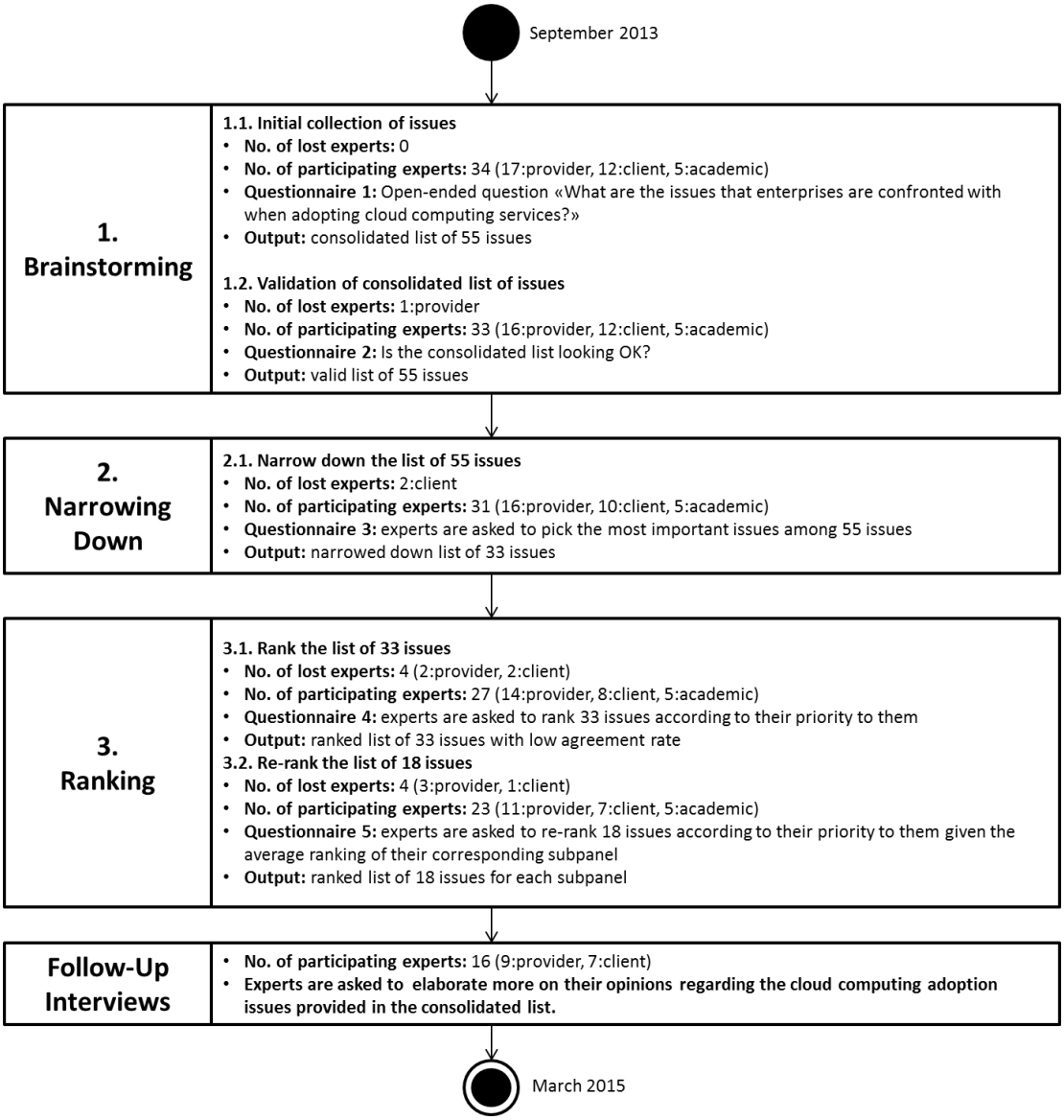


Figure 6: Overview of the Delphi study process

The experts' answers to the first questionnaire were analyzed and a consolidated list of 55 issues was generated (See Paper5 for the list). These 55 issues were grouped into 10 main categories. The analysis sought to identify the most important issues; through this work, similar issues were combined, and duplicate meanings were removed. My limited knowledge of the Norwegian language meant that, during the analysis of the answers to the first questionnaire, my supervisors assisted me with translation. Furthermore, my supervisors also checked the list after the analysis was completed.

Afterwards, we sent the consolidated list of 55 issues via e-mail to the experts to give their review and feedback. A deadline of one week was given to make sure that all their issues were analyzed, grouped and interpreted correctly by the researchers. This step is important to assure the validity of the consolidated list (Schmidt 1997). During this feedback round, we also had to send several weekly reminders to the experts to send back their feedback on the list. After this sub-stage, one expert withdrew from the provider subpanel; consequently, we were left with 16 experts on this subpanel. The majority of the experts accepted the consolidated list, and several reported that they found the results interesting. A few experts suggested some small adjustments to better clarify some of the issues.

A few experts from the provider subpanel provided some suggestions as to how to modify the list; for example, according to provider P4: *"It's ok. I think you have received some good and interesting input, but with that said I guess you need some further discussion, structuring and alignment. e.g. is your focus general or are you focusing on public cloud specifically? I think most of the inputs are related to public. If this study has a general focus I think it is important to distinguish between public, private and hybrid cloud. The characteristic of the different types of clouds are quite different especially when it comes to security. My view is if you make it too generic you will create an understanding that is over weighted about public clouds and security issues. Private and hybrid clouds provide a lot of security options at the same time as you keep most of the benefits from public clouds."*

Provider P6 also suggested some adjustments as to how to reformulate an issue about data security risks, which are not absolutes, but depend on some aspects: *"Some of the issues are formulated like absolutes while I think they are not. One example: the issue (It can be risky to move customer data to the cloud and it is preferable to be kept in-house) I do not agree that 'it is preferable to be kept in-house'. Sometimes it is safer to be stored in the cloud than in-house. This is dependent upon the provider, the*

agreements etc. My point is that Risks are not absolutes. Risks are to be dealt with and there are hopefully solutions on most risks (not all ☺). Just be careful in formulating the risks too narrow. I am OK with the list, it is covering my points."

Furthermore, the academic A3 suggested that the category of users be specified when talking about the meaning of cloud: *"Looks good. Just one minor issue. In the issue you talk about the meaning of cloud. I think this is very important from a management perspective - if managers do not understand what cloud is they won't use it. In your point, you talk about users, but are users then including management? This is not clear to me."*

Thus, the list was modified in a way that the provider, client and academic subpanels felt did not affect its agreed form. Furthermore, we now had a list of 55 issues that had been accepted by the panelists and was now ready for the narrowing-down phase.

In the narrowing-down phase, we sent the consolidated list of 55 issues as an online multiple choice survey form. This form was created using Google forms and featured check buttons and instructions for answering the survey. It was sent to 33 experts (a copy of this survey is included in Appendix B). We asked them to select 10 (minimum) to 20 (maximum) issues they felt were most important to them. They were given a one-week deadline. In this phase, each expert received a randomly arranged list of issues so as to avoid bias in the order of the listed items (Okoli & Pawlowski 2004). The response rate was low in the first week, with few experts submitting their answers to the questionnaire. Thus, we had to send several weekly reminders to those who had not responded. Eventually, we received answers from 31 experts on the second questionnaire, although two experts chose to withdraw from the client subpanel. Consequently, the size of the client subpanel was reduced to 10 experts.

Following this, we also received feedback from the experts that indicated their positive interest in the study. In particular, some of this feedback indicated a learning outcome from the experts' participation in the study. Client C13 stated his gains as follows: *"This has been very educational to me. I have been a cloud enthusiast for quite some time but I was looking at it mainly from the technical point of view due to the nature of my work experience. But now I am looking at cloud computing in a much broader and mature point of view."*

In the narrowing-down phase, the panelists' selection of the issues resulted in a list of 33 issues. By comparing the brainstorming (identification of issues) and narrowing-

down (selection of most important issues) phases, the observed trends per category were: (1) security (identified = 14 issues, selected = 11 issues); (2) availability (identified = one issue, selected = one issue); (3) migration (identified = three issues, selected = three issues); (4) business (identified = nine issues, selected = two issues); (5) legal and ethical (identified = seven issues, selected = five issues); (6) culture (identified = two issues, selected = one issue); (7) awareness (identified = four issues, selected = one issue); (8) impact (identified = seven issues, selected = five issues); (9) IT governance (identified = one issue, selected = one issue); and (10) strategy (identified = seven issues, selected = three issues).

The results of the analysis are displayed in graphs to make it easier for us to draw conclusions and select the issues that will be considered for ranking in the next phase. These graphs were sent to the experts in a report after the study had ended. However, during the study, a report that combines the votes of the three subpanels for each issue was sent to the experts along with the survey of the next phase. Client C4 from the client subpanel also asked us to share the report internally with the management: *"Can I distribute your documents to management […] as we are in the middle of making strategic choices related to CC now?"*

In the ranking phase, we sent a randomly arranged list of 33 issues to each of the 31 experts. They were asked to return their rankings within one week. This survey was created using the SurveyMonkey tool in the form of a list of rows that can be dragged up and down based on the priority given them (a copy of this survey is included in Appendix B). During the first week, we received five responses, thus, we had to send out three reminders, after which we received 27 responses in total. After this stage we lost four experts of whom two are from the client subpanel and two are from the provider subpanel. Consequently, we now had eight experts on the client subpanel and 14 experts on the provider subpanel. The results of the first ranking round were analyzed by calculating the Kendall's coefficient of concordance (W). We could not reach the level of concordance of W = 0.7 that is considered to be an indication of a high level of agreement for Delphi studies (Schmidt 1997).

Feedback comments from the first ranking round gave us an impression of the difficulties that arise when trying to rank too many issues, so by reducing the number of issues it was easier for the participants to focus on the issues most important to them. Furthermore, given that the Kendall's W values were very low, we decided to carry out a new ranking round based on a further narrowing down of the list of issues.

It was hoped that this would improve the Kendall's W values. As the first ranking round gave us an indication of which of the 33 issues were most important, it was easier to make a further reduction. Thus, we decided to focus on the top 18 issues, based on the mean ranking for each subpanel.

Since each subpanel had ranked the 33 issues quite differently, it was important to keep the top 18 issues for each subpanel. Thus, we cut the list of 33 issues into three different lists; each list contained the top 18 issues ranked by each subpanel. Three different lists of issues meant that it was not possible to calculate the Kendall's tau values to measure agreement among the three panels. Thus, we decided to focus on improving agreement within each subpanel instead.

In the second ranking round, we sent the eliminated list of 18 issues to each expert, along with the mean ranking of his or her subpanel and the panelists' comments from the previous ranking round. The survey was created in the form of an Excel file made up of three sheets. Sheet1 comprises an explanation of our reason for carrying out a second ranking round and instructions on answering the survey. Sheet2 comprised the survey in the form of a table, which showed the list of top 18 issues selected by each subpanel along with the mean rankings of the subpanel, the old ranking of the expert, and a space for placing the new ranking. Sheet3 contained experts' comments from the three subpanels; these were obtained from the first ranking round. A copy of this survey is included in Appendix B.

Each panelist was given the freedom to re-rank the issues or keep his or her old ranking, so long as it was within the range of 18 issues. We gave the panelists a deadline of one week to respond to the questionnaire; few responded during that week, so we had to send out several reminders to the remaining panelists. The second ranking questionnaire was sent to 27 experts, of whom 23 responded. Results from the two ranking rounds for each subpanel (academics, clients, and providers) are presented in detail in Paper5.

Some panelists emphasized that their ranking reflects their personal experience; thus, this may differ from other panelists within the same subpanel. Academic A1 stated that, *"Assessing these things is rather contextual, and depending on how one envisions the decision situation. For example, I was not overly concerned about security, because my experience is that while this obviously is a concern, it is one of the easiest to deal with."* Some panelists decided to keep their ranking, but only after adjusting their old ranking within the range from one to 18. For example, client C13 said: *"I*

stood by my old rankings (after revisiting them of course) because they were based on personal experiences that I have encountered which may not cover the full story behind cloud adoption or integration due to my role at each step of the survey [throughout the Delphi rounds]." Other panelists changed a few of their rankings for some issues and kept some of their old rankings for other issues. Furthermore, the response rate was slow in the last round and we started to lose more panelists.

This gave us an indication that it was unlikely we could continue for more rounds; hence, we decided to stop at this round and triangulate our findings with the data we collected from the follow-up interviews. Interviews were the second main data source for my study after the Delphi surveys.

The follow-up interviews took place in the period between the first and second rounds of ranking (June 2014 – September 2014), but they are placed at the end in Figure 6 for convenience. As I mentioned earlier, in Section 4.3, informants from the Delphi study gave inputs to the case studies through the follow-up interviews; however, some additional Egyptian informants were interviewed in late 2013. In sub-section 4.4.3, I present details on the interviews and the analysis of data that I collected from them. The Delphi study helped understanding the CC adoption as a social phenomenon in the context of the stakeholders' opinions and experience. To understand the phenomenon in its natural and setting and cultural context (Darke et al. 1998), two case studies were carried out.

4.4.2. Selection of Cases

"The individual researcher or research team must make their own choices in the light of their own context, preferences, opportunities and constraints."

(Walsham 2006, p.321)

The case study of Egypt

The choice of conducting an interpretive case study in the Egyptian context, to understand CC adoption phenomenon, was driven by three reasons. First, it is my home country. Second, it was undergoing radical socio-political transitions prior to and during the time of the data collection that was carried out from October 2013 to January 2014. Third, there is a limited knowledge in the existing literature about understanding the factors that affect CC adoption in Egypt. Before elaborating the aforementioned reasons in more details, I provide some figures from local and global reports on the status of Egypt as a developing country, its readiness and development

indices, as well as the initiatives that took place in realization of the challenges and opportunities related to CC adoption in Egypt.

Egypt as a developing country is experiencing economic and social development problems (e.g., rare job opportunities as well as increased unemployment and population growth rates) (UN 2002; UN 2012). It is also experiencing instability in its global ICT Development Index (IDI) in terms of access, use, and skills of ICT. Egypt recorded ranking progress from 91st in 2010, 87th in 2011, to 86th in 2012 worldwide in terms of access, use, and skills of ICT (ITU 2011; ITU 2013). However, there has been a noticeable move backward to the 89th place in 2013 and the 100th place in 2015 (ITU 2014; ITU 2015). Egypt recorded a backward move in ranking from 74th in 2010, 70th in 2011, 80th in 2012, 91st in 2013, to 94th in 2014, in terms of having the environment for ICT, readiness to use ICT, actual use of ICT, and impact of ICT on economy and society (Dutta et al. 2012; Bilbao-Osorio et al. 2013; Dutta & Mia 2011; Schwab & Eide 2014; Dutta et al. 2015; Schwab & Greenhill 2012). However, a recent report indicated that Egypt is among the economies that meet minimum requirements for basic CC services (Information Economy Report 2013). Thus, Egypt has the potential to benefit from the adoption of CC services (Shahin 2012).

For Egypt, CC is *"a technology priority which positively impacts the local economy in alignment with the global trend"* (MCIT 2013, p.24). CC is one of the strategic goals of Egypt's ICT strategy in the near and long future (MCIT 2013). This is manifested in the project initiative entitled "Supporting Information Technology Institute (ITI) Activities – Phase II" in 2011[2]. The responsible parties for this project are the MCIT[3] in Egypt as an implementing partner in collaboration with the ITI[4] in Egypt that operates by the MCIT and the United Nations Development Programme (UNDP) as responsible parties.

As a first step in this initiative, the ITI established the Egyptian Cloud Computing Center of Excellence (EC3)[5] in Assiut governorate. EC3 is a public private partnership among ITI, academia, and industry to place Egypt as a credible CSP in the global CC market as well as involve Egypt in research and development to explore aspects of CC.

[2] Collaboration project to promote innovation and entrepreneurship, develop professional calibers, and enhance international relations: http://www.undp.org/content/dam/undp/documents/projects/EGY/00060666/Pov_Pro%20Doc_ITI%20Phase%202.pdf

[3] http://www.mcit.gov.eg

[4] http://www.iti.gov.eg

[5] http://www.ec3-egypt.net

EC3 also provides SMEs with the resources to benefit from CC. Second step was training the staff of the EC3 and employees from private sector. Further, the ITI will seek to develop IT skills of university graduates through 9-month professional program initiative and arrange a job fairs event where private companies are put in contact with these graduates for internship and job opportunities. Third step involved promoting cooperation between ITI and national, regional, and international stakeholders with purpose of sharing knowledge among Egyptian and international professionals from organizations, training and legislative institutes, and universities. This cooperation takes place in the International Conference on ICT in Cairo called "Cairo ICT"[6] through sessions, tutorials, and technology and business exhibitions.

The Cairo ICT conference is organized by the ITI in cooperation with the Institute of Electrical and Electronic Engineers (IEEE). A series of sessions, workshops, and panel discussions have been held in the Cairo ICT conference in May 20th, 2013 under "cloud computing forum" theme. This involved discussions among stakeholders regarding the benefits from CC for Egypt and what challenges the new Egyptian government has to address in order to pave the way for CC adoption. The technological transition to the cloud requires thoughtful initiatives in order for Egypt to be legitimate in the widely growing market of CC. The connectivity problem needs a radical solution initiated by the Egyptian government to boost the telecommunications infrastructure. This was announced as a priority in the ICT strategy of Egypt by the minister of CIT in the Cairo ICT conference: *"we have to work on a set of trajectories to provide the technological infrastructure that enables us to attain these two strategic objectives [boosting the geographical position of Egypt as an international hub for the Internet and achieve social and economic development for the Egyptian society through ICT]. First, we need to provide the capable IT infrastructure that encompasses cloud computing, broadband, and submarine communications cables."*

According to one of the panel sessions in this event, a series of working groups sessions are planned, under the auspices of MCIT, to involve all stakeholders: CSPs and consulting firms representing expertise and potential adopters representing the 'needs', as CC adoption is going to be driven by these needs. One of the most critical issues in Egypt's journey to the cloud is the migration of business processes to the cloud, and potential adopters are cautious about this and need to gain knowledge about

[6] http://www.cairoict.com

best practices and successful stories in migrating to the cloud in order to draw their roadmap.

Regarding the use of social networking sites, especially Facebook, Egypt constitutes about a quarter of total Facebook users in the Arab region (Salem & Mourtada 2012). With 16 million users, Egypt is ranked first among the Arab region countries that use Facebook, and 17th worldwide in terms of audience size constituting 1.4% of global Facebook users (eMarketing Egypt 2013). Further, Twitter users in Egypt are not that many, approximately 519,000 users, compared to their Facebook equivalents (Report Arab Social Media 2013). This massive use of social media in Egypt is a consequence of the rapidly growing number of Internet users. A report by the Ministry of Communications and Information Technology (MCIT) in Egypt indicated that the number of Internet users was 38.75 million in December 2013 with Internet penetration of 45.93% (MCIT 2014a).

The first reason for selecting the case study of Egypt is that Egypt is my home country, thus, I had no language barriers in communicating with the informants. Thus, it was convenient for the informants to talk in Arabic and they were able to understand my questions. However, there was a major obstacle with the safety conditions that were quite instable at the time I started the data collection activities (i.e., there was a period of curfew that ended late November 2013). This situation was a consequence of the revolution that started in January 25th, 2011 and the violence activities as well as the radical political transitions that followed (Osman et al. 2011). This leads to the second reason for choosing Egypt case.

Egypt has undergone socio-political transitions, since the revolution, that had impact on all sectors in the country including the ICT sector. The 28th of January, 2011 was named "Friday of Anger", when all Internet connections and mobile phone communications were completely down because of the government order (Osman et al. 2011; Arthur 2011; Williams 2011). This threatened the public safety, safety of public and private properties, and the availability of Internet-based communication means. I have lived every single moment of the revolution and have witnessed its development before starting my PhD studies. After starting my PhD studies, I had a preconception that this revolution, based on my lived experience, would make influence on the adoption of CC in Egypt. However, as a researcher, I put this preconception aside when I started collecting the data and let it emerges from the interviews and the secondary sources. Example of informants' quotes indicated that

the Internet shutdown by the government had an impact on both CSPs and clients, as this threatens their business and affects their future trust in the government:

"Recently Egypt faced an Internet outage due to decree from the government which is not acceptable. We must have a law that prevents governments from forcing Internet providers to cut the Internet services as this becomes a very weak spot for cloud services trend in Egypt, all companies are now afraid of facing similar situation while depending on cloud computing. This will lead to outage and will impact the business."

(Provider P18)

"Internet cut in 2011 will always be a local fear in Egypt as it could happen again leaving business completely paralyzed."

(Provider P22)

One might think that this event (i.e., Internet shut down) that happened in 2011 was temporary and that life would come back to normal afterwards; however, this event had led to a long-term negative impression regarding the government. This is manifested in the abovementioned informants' quotes from December 2013 and January 2014.

The third reason for choosing Egypt case is the limited knowledge about factors that can affect CC adoption in Egypt. There is a limited body of research studies focusing on CC adoption in Egypt. The use of CC in Egypt is demonstrated in fields of web-based education and e-government. A survey study has been conducted by the British University in Egypt (BUE) to assess the effectiveness of using open source Moodle e-learning platform for improving the quality of students' comprehension, and the findings positively proved increased quality (Abou El-Seoud et al. 2013). For cloud e-government in Egypt, a study showed that the transition of e-government to cloud computing is not easy and has to be thoughtful; thus, the study proposed a "Before Cloud E-government" model or BCE-government model (Nasr & Galal-edeen 2012). The BCE-government model consists of five transition stages from Egyptian e-government to cloud computing: assessment, architecture re-construction, classification of services, aggregation, and legal contract. Another study proposed a hybrid model for adapting e-government to cloud computing in Egypt to minimize security, privacy, reliability, performance, and legal concerns (Hana 2013). This model consists of three clouds: (1) Intra-cloud that is a private cloud dedicated to a single national entity cluster, (2) Extra-cloud that is a community cloud that enables entities

from different clusters to integrate and aggregate their work as required, and (3) Inter-cloud that is a public cloud that enables users (i.e., citizens, guests, or organizations) to communicate with the government entities.

There is a need for focusing research endeavors on the limitations existing in developing countries that inhibit them from the development and use of ICT (Avgerou 2010). Furthermore, the use of theories is needed to understand how the socio-economic context enables or constrains the use of ICT innovations that improve life in developing countries (Avgerou 2010). This implicates the need for studying the role of political actors and institutions that provide basic infrastructures for ICT innovation and empowering societies (Avgerou 2010).

The case study of Norway

The choice of conducting an interpretive case study in the Norwegian context, to understand the CC adoption phenomenon, was driven by three reasons. First, the informants included in the case study of Norway were originally involved in the Delphi study rounds and accepted to participate in follow-up interviews. This explains the data collection period that started from May 2014 to September 2014, which is the same period of the Delphi follow-up interviews. Thus, the informants were easily accessible and language barriers could be overcome with the assistance of my Norwegian supervisors. Additionally, I had most of the client-side informants from the Norwegian public sector. Second, in addition to the thick descriptions that the informants provided for their answers to the brainstorming questionnaire and their reflections on the Delphi results, they provided interesting insights regarding the Norwegian context. Especially, the informants highlighted important events that influenced CC adoption decisions, such as the Narvik case and its consequences, the rigid municipal hierarchical structure, and the NSA surveillance and Norwegian CSPs. This second reason will be further elaborated after providing some figures from local and global reports on the status of Norway as a developed country, its readiness and development indices, as well as the initiatives that took place in realizing the opportunities and for meeting the challenges related to CC adoption in Norway.

Third, there is a limited knowledge in the existing literature about understanding the factors that affect CC adoption in Norway. A qualitative study explored enablers and inhibitors for adopting CC services in Norwegian organizations (Hustad & Olsen

2012). The study reported that cost saving, scalability, and elasticity are likely to attract Norwegian organizations towards adopting CC services. On the other hand, the study found that security risks, legal issues, integration hassle, and identity management issues are likely to inhibit the adoption of CC in Norway.

Norway was among the top 10 in 2011, 2012, 2013, and 2015 in the ICT development indices (ITU 2013; ITU 2012; ITU 2015). According to the Global Information Technology (GIT) reports of the past five years, Norway was among the top 10 advanced economies as being a ready society for ICT (Dutta et al. 2012; Bilbao-Osorio et al. 2013; Dutta & Mia 2011; Schwab & Eide 2014; Dutta et al. 2015; Schwab & Greenhill 2012). In terms of readiness for CC services, Norway is stated among the cloud prepared countries according to a recent report by Cisco (Cisco 2013). Norway meets the minimum requirements for advanced CC services in terms of having key cloud infrastructure indicators in place (i.e., hardware, network security, and Internet speed) (Information Economy Report 2013). Norway is considered as a promising market, both in the private and public sectors (Haeberlen et al. 2013). In 2011, 33% of the public sector and 38% of the private organizations adopted CC (Kristiansen 2011). This market has been responded by CSPs through the investment on a more reliable infrastructure, such as the capacity of data networks (Telenor 2013).

The Nordic vision towards CC is based on perceiving CC as a collaborative technology, which will drive innovation in the public sector through collaboration to gain new knowledge or achieve value-added ideas quickly (Frelle-Petersen et al. 2012). Thus, there will be no place for informational, procedural, and organizational islands. Common concerns reported among the Nordic public sectors are non-technological issues regarding transition to CC, legal issues regarding data protection, technical and organizational security, lack of governing the SLA, lack of interoperability, and challenges of integrating cloud solutions with legacy systems (Frelle-Petersen et al. 2012). Thus, the Nordic CC strategy should consider factors that enable and inhibit as well as articulate and communicate the IT maturity, infrastructure, and political needs along with expected benefits (Frelle-Petersen et al. 2012). Hence, the Nordic cooperation on CC focused on five key areas: (1) knowledge sharing, (2) regulations, (3) standardization, (4) procurement processes and tools, and (5) attracting datacenters (Frelle-Petersen et al. 2012).

Norway also has its own strategic initiative called ‘Digital Agenda for Norway’ that targets CC among other digital goals in addition to the aforementioned European and

Nordic initiatives (Ministry of Local Government and Modernization 2013; ENISA 2014). In this agenda, the Norwegian government foresees that CC services offer flexible and low-cost solutions for public and private sectors (Ministry of Local Government and Modernization 2013). Additionally, it has impact on creating jobs and businesses rapidly in Norway (Etro 2009). However, CC raises a serious conflict with the Norwegian legal requirements (Ministry of Local Government and Modernization 2013). This conflict comes from the fact that global CSPs have standard agreements that customers must sign, which do not meet data security and governance requirements stated in the Personal Data Act (Ministry of Local Government and Modernization 2013). These requirements stipulate that personal data may be stored in the EU/EEA area, with CSPs located in the United States who comply with the safe harbor privacy codes, or in other countries that protect the data in acceptable manner by the European Commission (Frelle-Petersen et al. 2012; Ministry of Local Government and Modernization 2013). Thus, the Ministry of Government Administration, Reform and Church Affairs will work on two key initiatives: (1) encourage public agencies to procure CC services, and (2) produce guidelines for the use of CC services to help clarifying relevant regulations as well as developing specifications and standard agreements for procuring CC services, as an alternative to the standard agreements currently used by CSPs (Ministry of Local Government and Modernization 2013).

CC adoption is still slow in the Norwegian public sector; this is attributed to the lack of experience and knowledge about CC among Norwegian organizations. This led 10 largest Norwegian municipalities to form a cooperation forum called K10 in collaboration with the Norwegian Association of Local and Regional Authorities (KS) to help speeding up the adoption of CC services in Norway (Hustad & Olsen 2012; Devoteam daVinci 2011). The purpose of K10 forum is to exchange knowledge about CC, establish common municipal ICT architecture, and influence ICT policies of public sector agencies (Hustad & Olsen 2012). Furthermore, it is argued that the adoption of CC services in Norway will be driven strategically by business value rather than economically by low-cost decisions (Hustad & Olsen 2012).

Despite the above enabling initiatives, the events and factors found in the case study had unlikely effects on CC adoption in Norway. The first event was in 2011, when Narvik municipality entered into an agreement with Google for using Google Apps without a clear sight on the location of the data (Gould 2012). In January of 2012, the Norwegian Data Protection Authority (Datatilsynet) banned the use of Google Apps.

Then, nine months later, this banning has ended and Datatilsynet became satisfied that Google certified its security of the data according to principles of safe harbor agreement (O'Donoghue 2012). However, this was not the only reason for ending the ban, as Datatilsynet had a concern about the U.S. Patriot Act and required Narvik to conduct risk assessment to get more information about data location, data segregation, and access controls, and Narvik did so (Gould 2012; Veum & Thoreid 2012). Moss municipality requested a review and guidelines from Datatilsynet for using Microsoft Office 365 (Veum & Nymoen 2012). Based on the review, these guidelines covered several sensitive areas, such as the agreement and data processing, segregation of personal data from different customer by Microsoft, security audits and risk assessments, access controls, storing logs for authorized and unauthorized use of the municipality's information system, and transfer of personal data. Since then, the use of CC services is restricted by conditional prerequisites (Datatilsynet 2012).

It should be noted that I did not have any clue about those two cases (i.e., Narvik and Moss) until I had an interview with P16. As a security consultant, P16 had PowerPoint slides which he used to present in workshops with clients. Some of his slides relate to the Norwegian law with regard to CC; one of his slides asserted on CC agreement issues, as municipalities cannot use the standard agreements offered by CSPs: *"If you have created a standard contract with a cloud service provider and store personal data, you most likely violate the Norwegian law"*. In his subsequent slides, he explains the Norwegian "Personopplysningslov" that protects the privacy of personal data during data processing; the law determines the responsibility of both data owner (i.e., the client) and data processor (i.e., the CSP). The data owner is obliged to ensure that the data are processed according to the Norwegian law. He also differentiated personal data (i.e., name and phone number) from sensitive personal data (i.e., health conditions and ethnic origins); each has to be treated differently. Afterwards, he exemplified with the cases of Narvik and Moss municipalities and their tough experience with CC and the Norwegian law. His point is to transfer the lessons learned from those two cases to the potential adopters of CC. He concluded his demonstration with some recommendations on how to use such services securely.

Furthermore, it should be noted that although these two cases were about adopting SaaS cloud services, the lessons learned from these cases are transferred to early and late adopters, additionally, the laws and guidelines enacted for adopting CC services are generally valid for all kinds of public CC services (i.e., either SaaS, PaaS, or IaaS).

"When they were finished with going through these cases [Narvik and Moss], we discovered three things that were very important: (1) that you [as a municipality] have to do, and it is required by the Norwegian law, risk analyses [before moving to the cloud]; (2) you have to have an agreement [called databehandleravtale] with the cloud service provider with specific needs according to the Norwegian law. So you cannot use the agreement directly from Microsoft…and Microsoft knows about it…and if you tell them that I cannot use your agreement because it is not according to the Norwegian law, so I have another agreement for you. They will say ok, it is fine, we know about it. So, you just come with your agreement and this agreement you should use is on the pages of Datatilsynet's home pages; (3) then you actually are required by the law to implement regular security audits of Microsoft if you choose Microsoft, and of Google if you choose Google. So Moss and Narvik, they now get information about security audits on Microsoft and Google. You need to get that information and you need to have those documents stored in your house to be in accordance with the Norwegian law."

(Provider P16)

Similarly, provider P17 highlighted the same stories of those municipalities and attributed this issue of complex laws and regulations to the fact that there are no good practices on how laws and regulations, at all levels (i.e., local, regional, and global), are interpreted. He mentioned: *"Regulations are complex […] when you have public cloud located in the US, you have some EU/US regulations and you have local legislation as well. So you are basically affected by, at least, two or three regulations at the same time and there is not a lot of practice in the area in terms of how to interpret the laws and regulations in various countries. […] If you look at two municipalities, in Norway, that moved to the public cloud last year, one to Microsoft and one to Google […] And they spent millions of kroners on lawyers in order to sort out the laws and regulations that they were affected by, by moving to the public cloud […] which is a good proof of complexity that they are affected by."*

The lesson for clients who are late adopters, such as C2 who planned for implementing a PaaS model privately, was that they started to be precautious about adopting public CC services and facing the situation where they dominate the new headlines for something wrong would happen.

It is worth mentioning that there were lessons learnt by the Norwegian legal system to upgrade and address the challenges brought by using CC services. In this regard, P16

mentioned: *"These two cases [Narvik and Moss] are what we need to look at and compare with for future cases because every detail of the law is not regulated because cloud services systems are new […] and there are so many new things for the Norwegian law and the court systems to go through, so they mainly take a few cases and they build [laws for the] next cases."*

It seemed that the cautiousness of clients to adhere to the Norwegian regulations opened a good opportunity for Norwegian CSPs. Thus, Norwegian CSPs represent a safe option for some clients to avoid being inspected about location of the data and guarantee adherence to the Norwegian regulations. In this regard, C11 asserted that they would contract a local CSP: *"The more local, the more safe according to regulations of the country's authority."*

A former study claimed that the key motive for adopting CC services in Norway is when the CSPs demonstrate successful stories of pioneer Norwegian client organizations adopting CC solutions and growing significantly (Hustad & Olsen 2012). However, it was found in the Norwegian case study I carried out that Norwegian CSPs tend to demonstrate their compliance with the Norwegian legislation and privacy regulations, and their physical storage of data in Norway. This conveys their independence of the Patriot Act and makes it a competitive advantage for them to grow in the cloud market. Thus, clients do not need to worry about the location of the data, as P12 asserted: *"I think that goes more back to the rules and regulations and where data are physically stored. I have seen that Norwegian cloud providers, especially backup services and those kinds of things have got a lot of attention lately because then you don't store data anywhere near the NSA."*

Clients in Norway are sensitive to the media, especially when the news headlines are occupied with Snowden leaks in 2013. Such an event has stopped a project for a client organization as expressed by P13: *"We struggled with that. We had the Snowden case which stopped a big project for moving all the business mailboxes in Norway. 30000 mailboxes were supposed to be moved into the Office 365 cloud, the project was stopped after all the headlines in the news with Edward Snowden saying that the US is reading [the] mailboxes, if you move them to Microsoft or to American companies, we have to stop this project. So now we are moving the mailboxes to another data server in Norway."*

A further context-related factor is the municipal hierarchical structure in Norway that is characterized by bureaucracy, which makes the decision-making process prolonged.

Especially, when there are conflicting interests between parties in the hierarchy. This was explained by C11 as a story of his municipality:

"We haven't a proper process around that yet. We have discussed it, but we haven't made any proper strategy around the cloud yet, mostly because of the data sensitivity. Where the data are stored […] If the data are stored in the USA, then we don't have the confidentiality. In our municipality, the main issue is to have a wider cooperation with all [small] municipalities to gather the main components in one place. When a decision matter or the IT department works on a proposal for a strategy, then it must be delivered to the administrative and then the executive, and then it is sent upward to the politicians to be agreed or to be decided whether to do that or not. Those small municipalities have also the same structure and they have different interests, goals, and knowledge about IT and use of IT systems. So our job here is quite a challenge […] Two years ago, I put up a small conference for all municipalities to discuss about CC and the vendors were invited two or three of them. We had a full day of discussion and presentations and none of the municipalities decided anything."

To sum up, the choice of the two case studies was driven by both opportunities and constraints as shown in Table 9. These opportunities and constraints were related to the time of conducting each study, familiarity with the context, communication (i.e., language), accessibility to informants, context-related events and factors, and the limited existing knowledge with regard to exploring factors that influence CC adoption in each context.

Table 9: Summary of reasons for the selected case studies

	Egyptian context	**Norwegian context**
Duration	October 2013 – January 2014	May 2014 – September 2014
Context attributes	-Among the top 100 countries in ICT development and ICT readiness indices -Meets minimum requirements for basic CC services -The main focus is on the technological infrastructure, acquiring knowledge, and socio-political instability before and at the time of the study	-Among the top 10 countries in ICT readiness indices -Meets minimum requirements for advanced CC services -The main focus is on the strict legal requirements and sensitivity to media news
Choice constraints	-Safety instability restricted me from having many face-to-face interviews	-Communicating with informants in Norwegian language was a barrier that I have overcome by supervisors' assistance
Choice	-My home country	-The informants included in the case are

	Egyptian context	Norwegian context
opportunities	-Easy to communicate with Arabic local language -Lack of studies that explore factors that affect CC adoption in Egypt	the ones who participated in the Delphi study; thus, they were easy to access and they provided insights on the Norwegian context -Limited studies that explored factors that affect CC adoption in Norway
Context-related factors and events	-Internet cut during the Egyptian revolution caused lack of trust from both clients and providers	-The cases of Narvik and Moss municipalities were influential -Snowden leaks in the media were influential -The hierarchical organizational structure of municipalities slows down the decision-making process

4.4.3. Interviews

"Not everything that counts can be counted, and not everything that can be counted counts"

-Albert Einstein

Interviews are the most important qualitative data gathering tool in qualitative research (Myers & Newman 2007). In this sub-section, I present the profile of the interviews, giving informants' codes, duration of interviews, mode of communication, dates of interviews, and their link to the Delphi study and/or the case studies (See Table 10). Furthermore, I indicate the inputs that these interviews provided to the Delphi study and/or the case studies. The reason that I repeat the columns DS, ECS, and NCS in Table 10 is that the overall contribution of the informants shown in Table 7 differs from their contribution through interviews. For instance, some informants took part in the Delphi surveys, but we lost them for the follow-up interviews, as was the case for informants P10 and C12. Informant P14 was interviewed as part of the case study of Egypt, but he also took part in the Delphi surveys; we lost him in the follow-up interviews and the second ranking round. The interviews were semi-structured, with a guide containing questions and themes. They combined open conversations related to the interview's focus in order to allow the informant a degree of freedom to express related matters not covered by the interview guide. A sample of key interview questions is provided in Appendix B.

After the Delphi surveys, each expert who responded to the ranking questionnaire was asked for a follow-up interview as a means of triangulation and to validate their input

to the study (Day & Bobeva 2005). We conducted 16 follow-up interviews in order to discuss the experts' responses in alignment with a summarized list capturing each subpanel's perspective on CC adoption issues. Furthermore, the interviews gave the experts an opportunity to further elaborate on their opinions about CC adoption issues and make bring greater clarity to the consolidated list of issues. In this regard, expert P6 said: *"it was good to have this interview because I was frustrated with the list and I felt I want to put my opinion into words out of the frame of the issues listed!"*.

We also wanted to involve informants from the provider and client subpanels to bridge the gap between the two groups. As client C1 stated: *"I hope your efforts are successful and you are able to bridge the gap that seriously exists between consultants, cloud service providers, and the customers"*.

In the case study of Norway, nine of the 16 follow-up interviews were used as main data sources, in addition to secondary data sources for triangulation (Eisenhardt 1989). Likewise, one interview out of the 16 follow-up interviews was used as a main data source in the case study of Egypt, in addition to 12 interviews and secondary data sources used for triangulation (Eisenhardt 1989).

The interviews took place through various communication means, ranging from face-to-face meetings and phone calls to online meetings and e-mails. In the case study of Norway, interviews were conducted synchronously.

In the case study of Egypt, I carried out six e-mail-based interviews and one phone interview followed by e-mails. The e-mail-based interviews were conducted for the informants' convenience, as they were too busy to be interviewed synchronously. They also found it easier to answer my interview questions in writing, when they had time to think and then write down their answers (James 2007; James & Busher 2006; Meho 2006).

Another reason for conducting e-mail based interviews was that few informants had their free time after working hours, which was late evening from 19:00 onwards. In late 2013 and early 2014, when this case study was carried out, the situation in Egypt was not stable or safe. Thus, e-mails were more convenient for the informants and the researcher. Furthermore, after the phone interview was transcribed, the follow-up process involved sending e-mails in order to clarify any points mentioned in the transcription.

Table 10: Interviews's profile

#	Informant's code	Communication mode	Duration	Date	DS	ECS	NCS
1	P1	Phone	28 m	10th June 2014	X		
2	P2	Face-to-face	1 h: 17 m	28th May 2013	X		
3	P4	Face-to-face	1 h	6th June 2014	X		
4	P6	Skype	53 m	29th August 2014	X		
5	P7	Face-to-face	37 m	12th August 2014	X		
6	P12	Skype	32 m	14th August 2014	X		X
7	P13	Face-to-face	56 m	24th June 2014	X		X
8	P14	Face-to-face	3 h	28th November 2013		X	
9	P15	Face-to-face	54 m	26th June 2014	X		
10	P16	Face-to-face	1 h: 29 m	23rd May 2014	X		X
11	C1	Skype	34 m	29th May 2014	X		
12	C2	Face-to-face	42 m	15th September 2014	X		X
13	C3						
14	C4	Microsoft Lync	44 m	15th August 2014	X		X
15	C5	Phone	23 m	18th June 2014	X		X
17	C9	Phone	25 m	26th August 2014	X		X
18	C11	Face-to-face	44 m	22nd August 2014	X		X
19	C13	Skype	37 m	29th August 2014	X	X	
20	P18	e-mail	-	2nd January 2014		X	
21	P19	e-mail	-	12th January 2014		X	
22	P20	e-mail	-	19th January 2014		X	
23	P21	e-mail	-	14th January 2014		X	
24	P22	e-mail	-	26th April 2014		X	
25	P23	Phone	22 m	17th December 2013		X	
26	P24	e-mail	-	14th January 2014		X	
27	P25	Phone followed by e-mails	36 m	14th January 2014 29th April 2014		X	
28	C14	Face-to-face	36 m	10th December 2013		X	
29	C15	Face-to-face	47 m	16th December 2013		X	
30	P26	Skype	1 h: 8 m	8th December 2013		X	

4.4.4. Secondary Data Sources

In addition to the interviews for the two case studies, I also used secondary data sources for triangulation to create connections between the findings from the interviews (Eisenhardt 1989). These secondary sources were related to each context, i.e., Egypt and Norway. I relied on a systematic review of the CC adoption literature before commencing my field work, which I discussed in Chapter 2 (See Section 2.4). Furthermore, I relied on the few examples of existing literature on CC and developing

countries for the case study of Egypt; this is in addition to the literature on CC and Egypt in terms of existing conceptual or empirical studies. For the case study of Norway, I relied on the existing literature on CC and Norway as well as on CC and the public sector, because it happened to include my Norwegian client's sample from the public sector. Additionally, I used several indexing reports, online news articles, PowerPoint presentations, official documents and reports that are published online, and video recordings. In Table 11, I demonstrate each type of secondary data source used and its purpose.

Table 11: Secondary data sources

Type of data source	**Description**	**Purpose**
Reports	-UNCTAD report for year 2013 -World economic forum reports for years 2011 up to 2014 (that provide networked readiness indexes) -ITU reports for years 2011 up to 2013 (that provide ICT development indexes) -Reports on adoption rates that are published in online articles and websites	-To get information about the readiness of both contexts Egypt and Norway -To get impression about the state of CC adoption in both contexts Egypt and Norway
Official online documents	-Guidelines and decisions made by the Norwegian Data Protection Authority (Datatilsynet) -Initiatives, yearbooks, statistics, and strategies published by the Ministry of Communications and Information Technology in Egypt (MCIT) -A document on MCIT's initiative in collaboration with UNDP	-To get more descriptions of and links to the interviews' data from both contexts Egypt and Norway (triangulation) -To report on significant external factors that influenced the adoption of CC in both contexts Egypt and Norway
Video recordings	-Videos for a series of key sessions that were held at Cairo ICT conference that is sponsored by the MCIT, major IT consultancies, and CC vendors and providers.	-To make links to the MCIT's initiative with UNDP and some interviews from Egypt case study (triangulation)
Online news articles, stories and case studies, and blogs	-This includes articles that were written about key events that had direct and indirect influence such as: o Narvik and Moss cases (Norway) o Internet shutdown during revolution (Egypt) o Announcements about plans and agendas as well as deals regarding CC adoption (Egypt and Norway) o Stories and case studies by major CC vendors and providers o Blog articles written by some informants whom I interviewed	-To get more descriptions of and links to the interviews' data from both contexts Egypt and Norway (triangulation)

Type of data source	Description	Purpose
Power point presentations	-Presentation were given by some Norwegian informants during interviews -Presentations available online by Norwegian informants whom I interviewed	-To get more descriptions of and links to the interviews' data from Norway case study (triangulation)

4.4.5. Data Analysis

"Findings emerge like an artistic mural created from collage-like pieces that make sense in new ways when seen and understood as part of a greater whole."

(Patton 2014, p.521)

With regard to the unit of analysis, this thesis is aimed at understanding CC adoption as a socially constructed phenomenon through capturing perceptible experiences (Heidegger 2005). Hence, my approach regarding the unit of analysis follows the phenomenological stance. I aim to understand the external and internal factors that influence the adoption and non-adoption of CC services. These factors belong to the broad societal environment, the surrounding business environment, and the internal environment of the potential or current client organization. In terms of data analysis, I followed the three concurrent activities proposed by Miles and Huberman (1994; 1984a): (1) data reduction (simplifying complex data through, for example, the extraction of recurring themes via manual coding (Patton 1990)); (2) data display (e.g., matrices, charts and graphs, and visual mapping (Langley 1999)); (3) and the drawing of conclusions (explaining the findings). I start by elaborating of the analysis of the Delphi's quantitative data, including the narrowing down criteria and Kendall's W of the mean rankings in each ranking round.

For the Delphi study, I coded the recurring themes in the experts' answers to the first Delphi survey. Data reduction activity was applied on the data from the Delphi study by excluding redundancies, which resulted in 55 CC adoption issues grouped into 10 categories. This list of 55 issues was later validated by the experts, and then reduced to 33 ranked issues. Then, the list was further reduced to three lists of the top 18 issues ranked by each subpanel.

It should be noted that there are some contextualization points related to the Delphi study that I will highlight in the subsequent paragraphs. The approach that I have taken was to explore, develop and rank a list of CC adoption issues to seek qualitative inputs

from the panelists based on their personal judgment and subjective views (i.e., opinions). These opinions are a result of their experience. The panelists' opinions have also provided relational and contextual representations of the highly ranked issues without any pre-classifications (Linstone & Turoff 1975). In Delphi studies, the *"evidence must necessarily be gathered through observation of people and the context for their actions"* (Day & Bobeva 2005, p.108). Hence, it was appropriate to solicit the panelists' opinions based on their domain backgrounds and personal experience as clients, providers, and academics to contextualize the findings of the Delphi study.

Since the purpose of the Delphi study was to explore CC adoption issues that confront enterprises, the study started with a broader scope on those issues and we preferred not to contextualize them based on prior knowledge, rather, as the study progressed with feedback from and interviews with the panelists, these issues have been contextualized by the panelists. For instance, one of the issues was related to security risks, and the statement was broad in the consolidated list before the feedback round. After the feedback round, some panelists suggest to contextualize this issue by clarifying that security risk as high in public clouds and low in private clouds, as illustrated in Figure 7 and Figure 8.

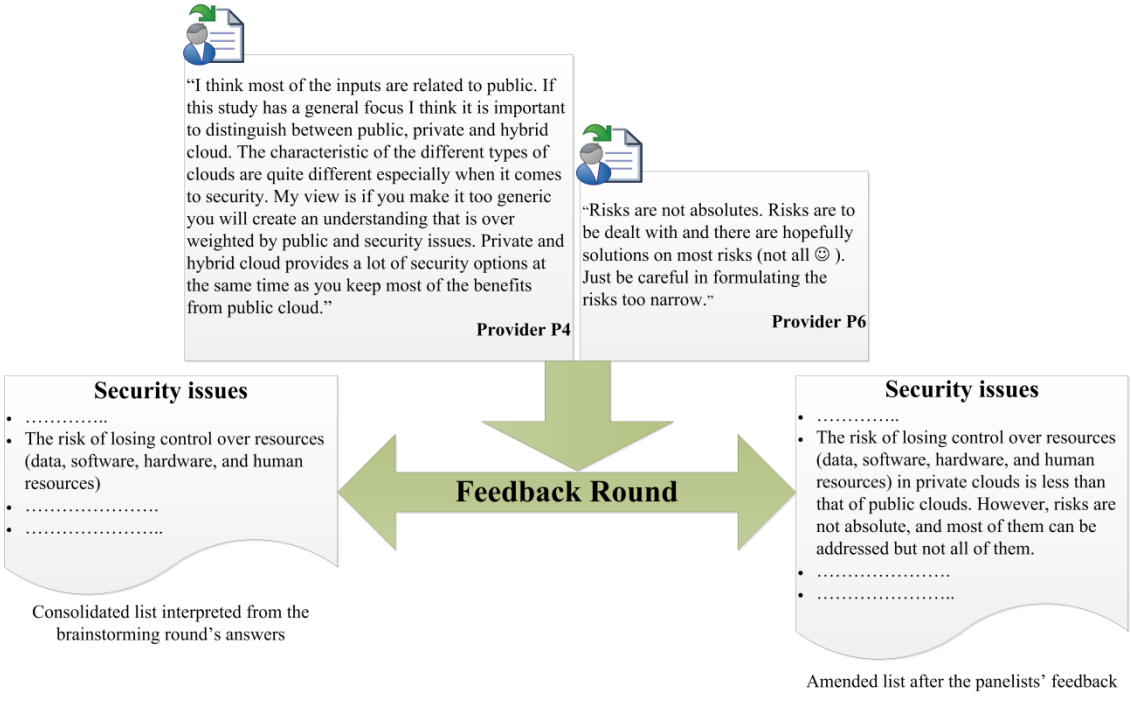


Figure 7: Example (1) of analyzing the Delphi's list of 55 issues based on the feedback round

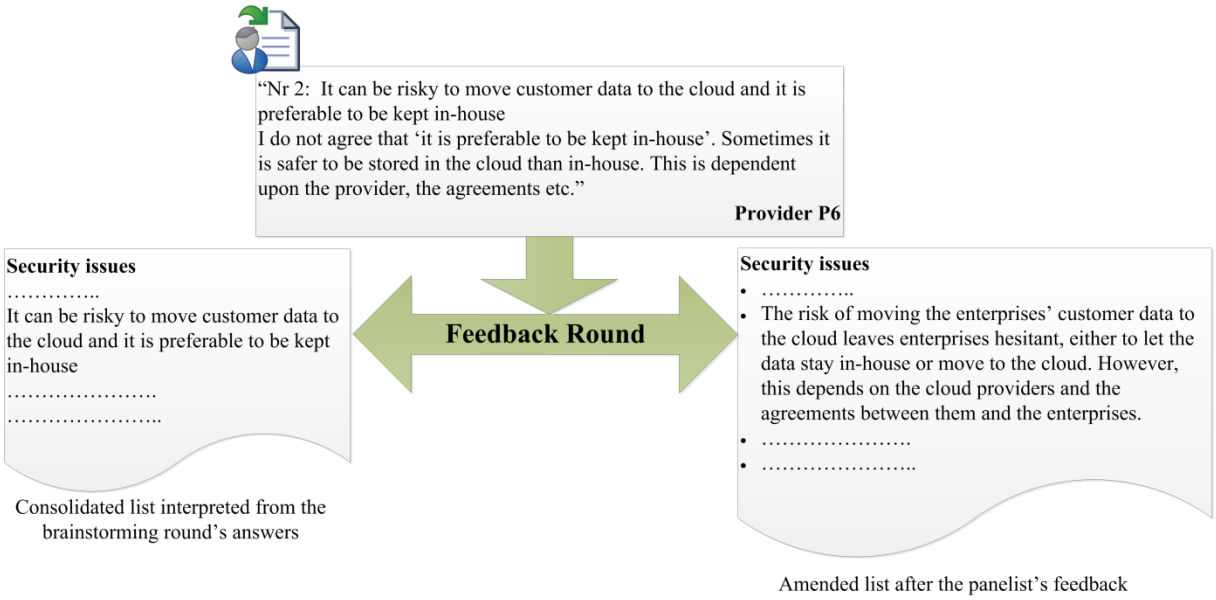


Figure 8: Example (2) of analyzing the Delphi's list of 55 issues based on the feedback round

In the narrowing-down phase, we chose to analyze the votes of each subpanel separately. In particular, we noticed differences between the subpanels in the way they prioritized the issues and, thus, we wanted to highlight these differences. The analysis of responses from this phase involved calculating the votes that each issue gained from each of the three subpanels. Then, we calculated the percentage of total votes gained for each issue per subpanel. Our intention was to narrow down the list to a more manageable list of issues; 15 issues at the least and 20 at the most. In this regard, we adopted the strategy of picking issues that gained votes about 50%, as a threshold, by the panelists in each subpanel, which resulted in a short list of 12 issues out of 55. We were concerned that important issues may be omitted; thus, in order to be left with a reasonable list, we decided to use 30% as a possible threshold. The narrowing-down resulted in a list of 33 issues ready for ranking. We decided not to further reduce the number of issues using an arbitrary strategy, because it is the role of the experts, not the researchers, to select the most important issues (Schmidt 1997).

The results from the first ranking round were analyzed by calculating the mean ranking for each subpanel and the Kendall's coefficient of concordance (W) for their rankings of the 33 issues. This was carried out using SPSS software. Kendall's W values are calculated in order to measure the degree of consensus among the experts in each subpanel. The level of agreement among panelists in each subpanel was below 0.7, which, according to Schmidt (1997), indicated a very weak agreement. The highest value of W was found within the academic subpanel (N=5 academics, W=0.270, sign=0.089), then the client subpanel (N=8 clients, W=0.173, sign=0.072).

The lowest value was found within the provider subpanel (N=14 providers, W=0.069, sign=0.533) (the detailed results can be found in Paper5).

The results from the second ranking round were analyzed by calculating the mean ranking and Kendall's W values for each subpanel using SPSS software. In general, there was an improved degree of agreement within each subpanel compared with the first ranking results. The highest W value was among the academics (N=5 academics, W=0.493, sign=0.001). However, there was an improved and significant degree of agreement (although still not high) among the clients (N=7 clients, W=0.392, sign=0.000), and the providers (N=11 providers, W=0.443, sign=0.000).

Along with data reduction activity, data display activity is applied through making graphs to demonstrate the votes that each CC adoption issue gained from each subpanel in the Delphi study. This helped in the drawing of conclusions when narrowing down the list from 55 issues to 33 issues. The 33 issues were then sorted into tables along with their average ranking. This helped in the drawing of conclusions when focusing on the top 18 issues for each subpanel. The same procedure was followed for the re-ranking round. The 18 issues were sorted into tables along with their average ranking, and this gave an indication of the variations in the order of the issues between the first and second ranking rounds. I was then able to draw conclusions and create relationships regarding the most commonly top ranked issues across the three subpanels, and link them to the coded follow-up interviews' transcriptions to provide thick descriptions for the top ranked CC adoption issues.

The identified issues from the Delphi study have been interpreted differently by clients, providers, and academics. Some issues have been overlooked by the clients and highlighted by the providers and academics, and vice versa. For instance, the security issue: "Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for" was given the highest priority by clients (ranked number two), and much lower by providers (ranked number 17) and academics (ranked number 11).

For the two case studies, recorded interviews were transcribed and the textual content of the interviews, together with the content of e-mail-based interviews, was coded using concepts from neo-institutional theory (i.e., three isomorphic pressures and five strategic responses, as explained in Chapter 3, Section 3.1). Furthermore, the reasons behind each strategic response were coded using simple terms. Examples for sample

codes of interview quotes are provided in Table 12. The analysis of the secondary data was useful for making links between the coded themes from the interviews.

Table 12: Sample codes of interview quotes

Quotes	Codes
"Starting with security perspective, if IT decision makers do not understand the implications of giving away their data to cloud providers, then that can make it hard to adopt the services."	Transparency
"SLAs or at least the ones we got are written by lawyer for lawyers; so a simple business manager, I am pretty sure, will find […] some more troubles in understanding the complete reach of the SLA with the current cloud providers."	Understandability
"The underlying fundamental reason was a strategic drive towards outsourcing and making the internal organization leaner, so that was the main drive, but in that entire process we missed out on 'whether we are ready for the cloud or not?!' so that's what we lacked!"	Immaturity
"You have to do, and it is required by the Norwegian law, risk analyses […] and then you have to do it after; this is required. And you have to have an agreement with the cloud service provider with specific needs according to the Norwegian law"	Coercive pressure
"Why do I need cloud […] to dynamically adjust or adapt to the workload depending on my requirements […] instead of having a data center and buying hardware and I don't have proper capacity planning for my requirements […] the public cloud provides this in much more accurate way, say I bought a virtual machine and I will pay for it while it is up and running, and if I shut it down, I will not pay a single penny. For a decision-maker, this is a dream! It is like renting hardware and no need to do upgrading or maintain license. And if the load increased, updating the specs can be done on the fly […] this is why do we need to move to the cloud to become more agile and more flexible, and maintain our costs."	Agility Efficiency
"There are various cloud computing business models, will be discussed in detail, that offer competitive advantages for all users including large, small, and micro enterprises. This seminar will be followed by a number of workshops arranged under the auspices of MCIT and run by participating partners from national and international companies to understand the potential of cloud computing applications in the Egyptian market. I hope that all parties including national and international companies, ministries' representatives, or other institutions in all sectors collaborate together to achieve fruitful outcomes from this forum. I expect that this will result in absorbing experiences from international companies and gaining maximum benefits."	Normative pressure
"No, because it is not clear what are the gains because it requires a lot and there is this issue of confidentiality. *I have a kind of difficulty to give you a clear enough answer because I suppose we are still unclear ourselves."*	Security Unclear vision

Now, I will provide examples of codes and data analysis procedures I followed to analyze the data from the Delphi study and two case studies to arrive at the institutional factors and CC adoption strategies identified in this thesis. A general procedure I followed in the data analysis process was that I linked qualitative and quantitative data for the purpose of triangulation and providing an elaborated analysis with rich details, which offered fresh insight (Miles & Huberman 1994). The data analysis involved revisiting and re-interpreting the empirical results; this is done by combining results from the two case studies with the Delphi's results and the literature. In Figure 9, I provide an overview of the linkage I made between the data to reach the findings.

"Qualitative analysis transforms data into findings. No formula exists for that transformation. Guidance, yes. But no recipe. Direction can and will be offered, but the final destination remains unique for each inquirer, known only when—and if—arrived at"

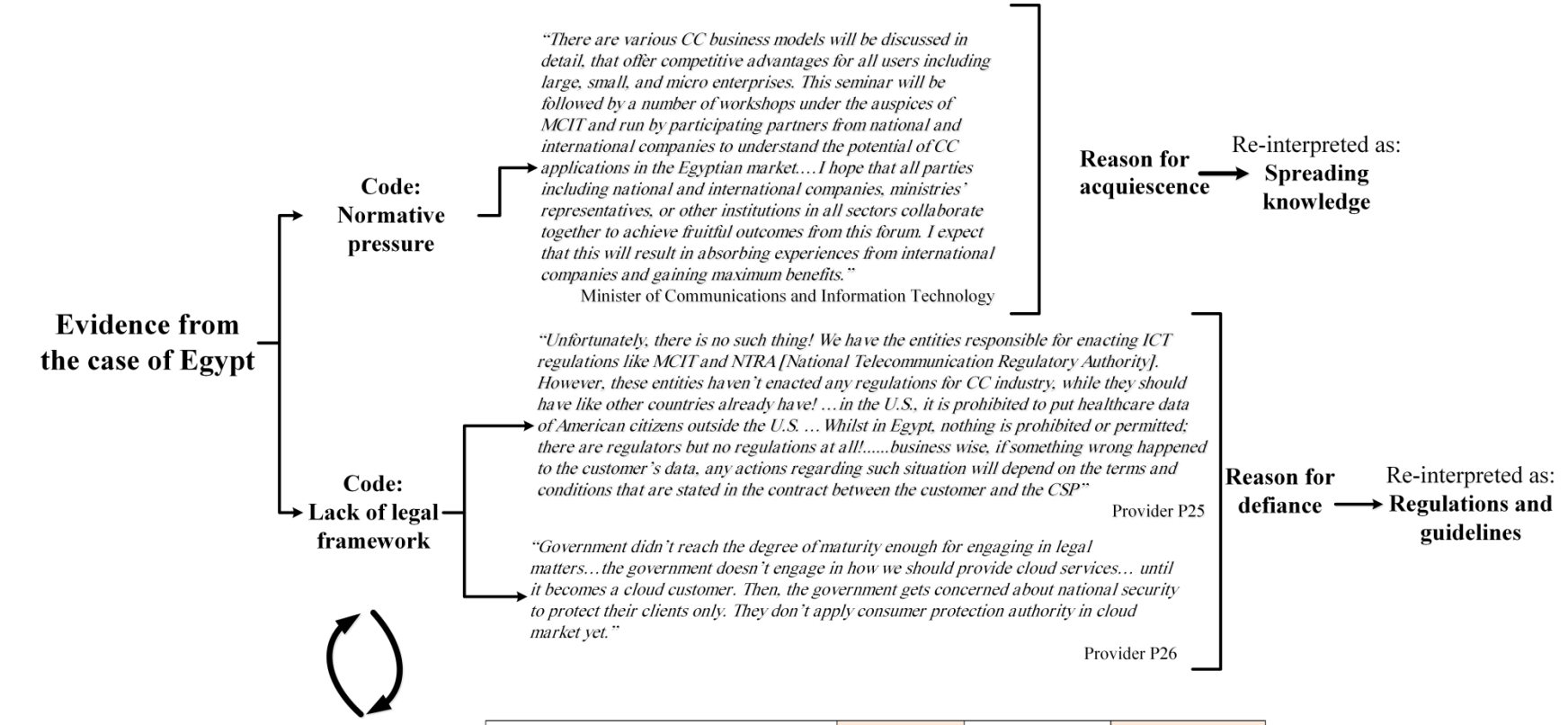
(Patton 2014, p.521)

In the rest of this Section, I will provide examples of how the quantitative data (i.e., rankings) and qualitative data (i.e., interviews and documents) supported the derived findings that constituted the contribution of this thesis. First, I adopted the visual mapping as a sensemaking strategy (Langley 1999). I analyzed the data in a visual form using graphical shapes and tables (Miles & Huberman 1994). Furthermore, it should be noted that *"there is a step in the connecting of data and theory that escapes any deliberate sensemaking strategy a researcher might decide to apply"*, and this *"uncodifiable"* step *"relies on the insight and imagination of the researcher"* (Langley 1999, p.707), because *"we just do not know and cannot tell where that critical insight came from"* (Langley 1999, p.708). Second, I followed the fundamental principle of the hermeneutic circle, which follows that the understanding of a complex whole (i.e., CC adoption factors and strategies) is achieved by iterating between the meanings of its parts (i.e., data collected from different sources and methods such as Delphi rankings, interviews, and secondary sources) and their interrelationship (Klein & Myers 1999).

Figure 9: Data analysis procedures followed

Despite the research questions raised in this thesis have a wide scope; the answers were related to particular contexts, since the context is important for the interpretive research (Walsham 2006) and *"it is the particularities that produce the generalities, not the reverse"* (Miles & Huberman 1994, p.35).

For the purpose of manageability and plausibility regarding the research focus, the data reduction procedure was applied to select, focus, simplify, and transform the data collected (Miles & Huberman 1994) (Halperin & Heath 2012). Data reduction involved discarding redundancies, especially in generating the consolidated list from the Delphi brainstorming questionnaire. The data reduction also involved selecting *"the most interesting and compelling statements concerning"* the focus of the study (Halperin & Heath 2012, p.279). The selection involved comparing the data from interviews and secondary sources with the Delphi rankings and the gap in the CC literature. Transformation of the data involved coding using themes from the neo-institutional theory and open coding in some cases. In the following, I provide examples from the analysis of the data (Figure 10, 11 and 12). Further analysis examples are provided in Appendix B.



Issues (Legal and Ethical)	Client rankings	Provider rankings	Academic rankings
Data protection legislation is different and not strong in all countries.	1	10	3
Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.	5	11	4

Figure 10: Analysis example 1

Figure 11: Analysis example 2

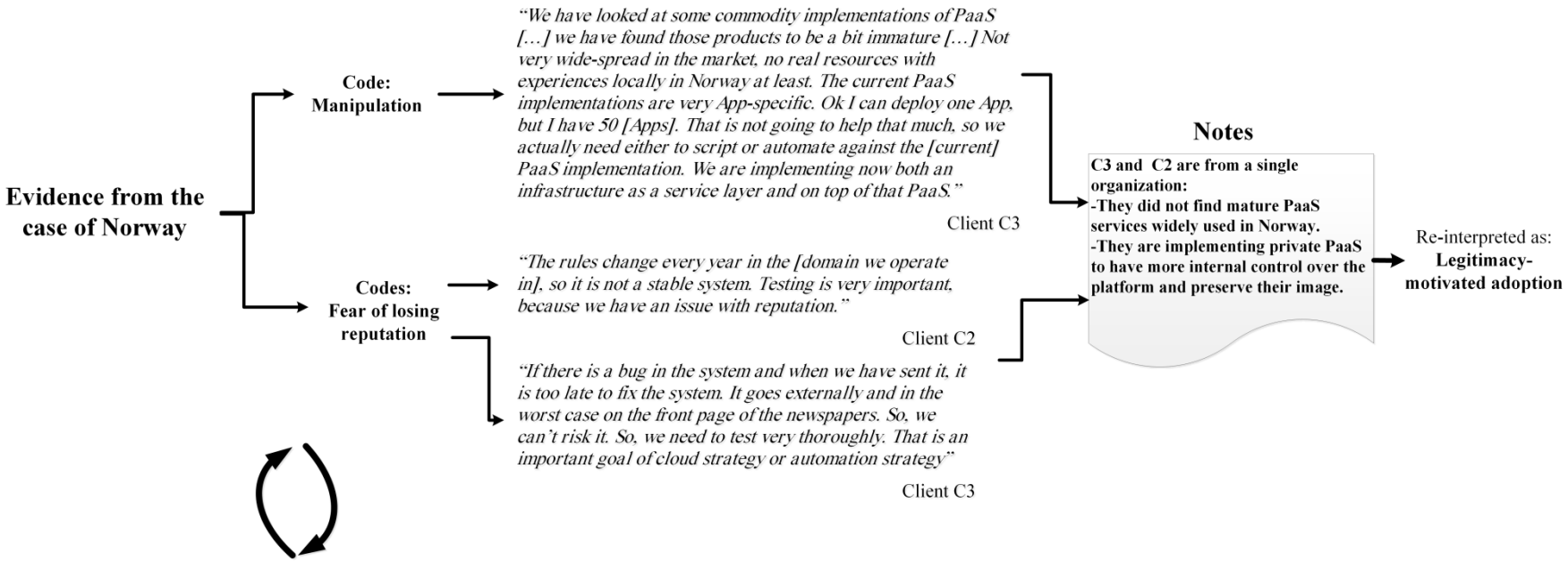


Figure 12: Analysis example 3

CC Literature →

Existing studies have focused extensively on various factors that determine cloud sourcing decisions (Schneider & Sunyaev 2014); such a focus has been more on the technical than the institutional factors (Yang & Tate 2012; Schneider & Sunyaev 2014). The literature also focused on readiness assessment (Loebbecke et al. 2012), capabilities offered by CC (Iyer & Henderson 2012; Iyer & Henderson 2010), and practices to overcome CC adoption challenges, such as educating stakeholders, matching CC services to existing needs, finding the right CSP, and building client-provider relationships, and acquiring the adequate skills (Lacity & Reynolds 2014). There is less focus on how various CC adoption strategies are shaped by combinations of institutional factors that are related to a wider social system of various involved parties.

4.5. Validity Issues

In this section, I describe the validity issues associated with my research approach, including matters related to the Delphi study and the two case studies.

Unlike traditional surveys that aim to generalize the results to a larger population and to prove statistically significant effects in the populations, sample representativeness in the Delphi study method is quite different and complicated and might also be questionable, since the Delphi study aims to gain consensus of opinion regarding issues connected to decision-making from a group of experts (Okoli & Pawlowski 2004).

There are discrepant schools of thought regarding the sufficient Delphi group size; some literature suggested 10 to 18 experts as sufficient for a Delphi panel (Okoli & Pawlowski 2004). On the other hand, some other literature sources indicated that there is a lack of a widely agreed standard for the sample size of Delphi studies, and it is more researcher and situation specific (Akins et al. 2005).

There have been Delphi studies with sample size starting from five experts (Akins et al. 2005). The academic subpanel in this Delphi study consisted of five experts which is a limited number, however, acceptable according to Akins (2005). The academic participants contributed with important perspectives on CC topics that became valuable in the analysis.

As mentioned in Section 4.3, 34 experts contributed to the Delphi study. The experts had various domain backgrounds (i.e., clients, providers, and academics) and from various industries, sectors, and countries. However, the experts were distributed into three subpanels according to their domain backgrounds as stakeholders (i.e., clients=12, providers=17, and academics=5). Because I had few experts from each country, it was not appropriate to divide the experts into subpanels based on their countries.

In addition, doing a cultural comparison was not an analytical option for some of the countries since only one expert participated per country, which was the case for UK and Finland. For some of the other countries, I had only two experts per country, such as USA, Egypt, and Pakistan. The following Table 13 illustrates the number of experts within each subpanel, organized by stakeholders group and by country.

Table 13: Distribution of panelists by stakeholders group and by country

Stakeholders\Countries	**USA N=2**	**UK N=1**	**Norway N=26**	**Finland N=1**	**Egypt N=2**	**Pakistan N=2**
Clients N=12			10			2
Providers N=17	2	1	11	1	2	
Academics N=5			5			

During the time between each Delphi round some panelists changed their jobs, knowledge and situational context (Day & Bobeva 2005); they had a mixed experience, both as a client and a provider. For instance, C13 whose role was an infrastructure administrator for a client organization at the time of the brainstorming round (which started in September 2013), then he changed his job to a technology solutions professional for a CSP at the time of the narrowing down round (which started in January 2014), and then he later switched to a system engineer for another CSP at the time of the two ranking rounds (which started in April 2014 and February 2015). This is asserted by C13 after he submitted his answer to the last ranking survey: *"I stood by my old rankings (after revisiting them of course) because they were based on personal experiences that I have encountered which may not cover the full story behind cloud adoption or integration due to my role at each step of the survey."*

Hence, the opinion based on the personal experience, and even mixed experience, of each panelist helped to contextualize the findings of the Delphi study, rather than the country of the panelists. Furthermore, some informants from the case study of Egypt had this mixed experience prior to the interviews (e.g., informant P21 and P25).

Like any qualitative interpretive research study where biases are unavoidable, this study is not free of the researcher's or informant's bias during the course of data collection and analysis (Darke et al. 1998). In interpretive research, *"our theories concerning reality are ways of making sense of the world, and shared meanings are a form of inter-subjectivity rather than objectivity"* (Walsham 2006, p.320). However, to improve the accuracy, credibility, and construct validity of the empirical descriptions of my study (Yin 2009), I adopted two techniques:

1. Triangulation using multiple sources of evidence; I used secondary data sources (See Table 11 in Section 4.4.4) as a means of triangulation to enrich my

understanding of the contextual issues from the two cases, and to make links between the information from the secondary sources and the stories from the informants as well as the issues emerged from the Delphi study.

2. The researcher's interpretations of the findings were checked with members of stakeholders from whom the original data was collected (Bygstad & Munkvold 2010). This was done to validate the correctness and meaningfulness of the researcher's analysis. In the Delphi study, as elaborated in details in sub-section 4.4.1, I requested the informants' feedback on the consolidated list that I generated from their answers to the brainstorming questionnaire. Some informants from provided feedback comments to correct some listed issues; thus, the consolidated list was corrected accordingly (Franklin & Hart 2007). Furthermore, the follow-up interviews were mainly around discussing the consolidated list and their individual answers to the brainstorming questionnaire. Additionally, in the second ranking round, the informants were provided with comments stated in the first ranking round from some other informants. Thus, they were given the opportunity to read those comments, provide feedback on the average rankings of their corresponding subpanel, and compare the average with their own rankings.

In the narrowing down round, I generated a random list of issues not to affect the choice of informants when picking the most important issues (Okoli & Pawlowski 2004). Similarly, I sent a random list of narrowed down issues to the informants in the first ranking round to eliminate the bias (Okoli & Pawlowski 2004).

To eliminate the informant's bias, the questionnaires were sent to each panelist in a separate e-mail to reduce the effect of dominant individuals (Dalkey 1972). However, in order to improve the agreement level within each subpanel in the second ranking round according to the method (Okoli & Pawlowski 2004), each informant was asked to revise his/her old rankings in light of the average rankings of their corresponding subpanels and the comments from the previous ranking round. This was seen by the client C11 as a way of influencing his rankings*: "I think it was not correct to let the client see the average rankings. I'd rather [do] my own ranking in the order from 1 to 18 within those issues."* However, I explained to the panelist that, methodologically, sharing the average ranking of the subpanel is for the purpose of gaining consensus among the panelists (Okoli & Pawlowski 2004).

In the case study of Egypt, I had e-mail based interviews with some informants; however, I had subsequent discussions with them through e-mail to get more clarifications of what I understood from their previous inputs (Meho 2006; James & Busher 2006). Similarly, I had an e-mail discussion with an informant, whom I had a phone interview with.

I experienced language barriers during the data collection course, especially with the Norwegian informants as I elaborated in details in Section 4.1. For researchers conducting field research away from their own country, it is preferred to know the local language of that foreign country, which is not possible in all cases and professional translators would be expensive and not knowledgeable about my research topic (Walsham 2006). When interviewing the Norwegian informants, the language was an obstacle in some interviews, but not all of them. Some informants were able to express their experiences in English, whilst others were not. I overcame part of this challenge by conducting the interviews with the assistance of my supervisors, and when necessary; they collaborated with me during the Delphi study and attended some of the interviews, and had knowledge about my topic (Walsham 2006). When transcribing the interviews, my supervisors also assisted in translating parts that included a Norwegian quote. They also assisted in translating Norwegian answers to the first Delphi questionnaire and comments throughout the Delphi questionnaires. However, on some occasions, I had to conduct some interviews with Norwegian informants by myself; these informants would prefer to speak in Norwegian. Consequently, I tried to simplify the questions for the informants, and they tried to convey their story and experience in English in a way that I could understand.

There are discrepant views with regard to the generalizability from Delphi results to other settings and contexts. One view demonstrates the plausibility of generalizing from Delphi results, which follows that researchers can utilize the wide range of experts' opinions and experiences to *"significantly extend the empirical observations upon which their initial theory is based—thus strengthening the grounding of the theory and increasing the likelihood that the resulting theory will hold across multiple contexts and settings."* (Okoli & Pawlowski 2004, p.15). However, another view suggested that due to the small number of experts involved in Delphi studies, *"Delphis do not (and are not intended to) produce statistically significant results; in other words, the results provided by any panel do not predict the response of a larger population or even a different Delphi panel. They represent the synthesis of opinion of the particular group, no more, no less. The value of the Delphi method rests with the*

ideas it generates, both those that evoke consensus and those that do not. The arguments for the extreme positions also represent a useful product" (Gordon 1994, pp.3–4). Both views hold for my view on the generalizability from the Delphi study results. For instance, the empirical results from the Delphi study indicated that security is the overarching issue among CC adopting issues identified. This finding extends the assumptions in the literature and implies that security concerns hold across multiple contexts. Hence, Okoli and Pawlowski's (2004) view holds for the Delphi results. Additionally, the Delphi study provided rich explanations of various aspects of security, which extended the previous empirical observations regarding security. These explanations generated interesting perspectives about what constitutes the security issues in addition to the resulted top rankings, despite a high consensus was not reached. Hence, Gordon's (1994) view holds for the Delphi results.

The validity issues of the Delphi results are demonstrated in Table 14 according to the evaluation criteria suggested by Day & Bobeva (2005):

Table 14: Validity issues of the Delphi study

Evaluation criteria	**Description**
Confidence levels	Being a researcher: • I acted purely as a facilitator of the Delphi rounds and not a participant (i.e., sending questionnaires to the panelists, clarifying panelists' inquiries, and send reminders to the panelists). • I was careful about my subjective interpretations of the consolidated list; thus, the list has been validated by the panelists during a controlled feedback round after the brainstorming round. Furthermore, the panelists were given the freedom to post comments/justifications when choosing the most important issues, ranking and re-ranking them, as the *"failure to understand the context for the consensus may lead to subsequent failure to capture important contextual information"* (Day & Bobeva 2005, p.112). • In the narrowing down round, the most important issues were selected based on their gained votes with 30% threshold. After the first ranking round, the list of issues was further narrowed down into the top 18 issues based on the average rankings of each subpanel. • The intra agreement among the panelists within each subpanel was measured through running the nonparametric statistical technique Kendall's W, as statistical analyses eliminate bias (Hsu & Sandford 2007). • The psychological factors that cause random and systematic errors impacting the study are difficult to detect and could be acknowledged (i.e., work pressures, the time when the survey was completed, or the mood of the informant) (Day & Bobeva 2005).

	This might have happened when reviewing the consolidated list of 55 issues, choosing the most important issues among the 55, ranking the 33 issues, and re-ranking the 18 issues.
Rigour	• The feedback comments from the panelists on the consolidated list are received, acknowledged and reflected properly in the list, especially comments that entailed contextual changes.
Credibility	• Follow-up interviews with some clients and providers were conducted as a means of triangulation to provide more descriptions on the issues identified. • Various perspectives have emerged across the subpanels, from the rankings and interviews, which could be attributed to the different contextual settings of the individual panelists (i.e., domain background, job title, or country). • The generalizability of the Delphi results to another context is limited and does not, statistically, represent a larger population due to the small number of panelists involved. Rather, the results provided a synthesis of opinion of a particular group (i.e., clients, providers, and academics) and debatable consensus patterns.

I further demonstrate, in Table 15, the degree to which my research approach complies with the principles for interpretive field research in IS (Klein & Myers 1999).

Table 15: A summary of the validity issues according to principles for IS interpretive research

The principle	**Its applicability to this research**
1. The fundamental principle of the hermeneutic circle	There were several iterations between the parts, which are the collected data (responses to Delphi surveys, informants' interviews, and documents) and literature, theory, and the whole "CC adoption phenomenon".
2. The principle of contextualization	The understanding of CC adoption took place within its social and historical settings such as historical events at the social level in the case study of Egypt such as the revolution event, and in the Narvik and Moss cases that provided a turning point in the Norwegian context.
3. The principle of interaction between the researchers and the subjects	The social construction of the data took place in the interaction between the researcher as an outside observer and the informants, which can be a limitation compared to being an insider. I mean by the outside observer that the personnel in the field organization viewed me as an 'outsider'; additionally, I was not engaged in many occasions and I had no direct sense of the field organization from the inside (Walsham 1995).
4. The principle of abstraction and generalization	The data interpretations from the case studies were linked to concepts from the neo-institutional theory that was introduced in Chapter 3. For the Delphi study, the researcher coded the data and drew relationships between the themes without using theory. Then, the data was reinterpreted after writing the papers. This interpretation involved the generation of relationships between the theoretical concepts and the emerging themes from the Delphi

The principle	Its applicability to this research
	study, and constitutes the contribution of this thesis.
5. The principle of dialogical reasoning	Before commencing data collection activities, I had a pre-understanding of CC adoption and neo-institutional theory from the literature. I used simple terms during the interviews so that informants can understand. As the data collection proceeded, my understanding of the emerging themes from the data led me to use the theoretical concepts to interpret the data. Then, new interpretations led to reaching new concepts that helped me understand the phenomenon of CC adoption.
6. The principle of multiple interpretations	The informants provided various interpretations and experiences with the phenomenon of CC adoption (e.g., security in the cloud is interpreted by clients as a risk, while providers interpreted it as a competence). To some extent, the institutional factors varied from one context to another. Consequently, I tried to provide logical explanations during the data analysis.
7. The principle of suspicion	To avoid creating biases in the collected data, the list of CC adoption issues generated during the Delphi study was reordered for each expert in each Delphi questionnaires. Furthermore, the consolidated list of issues resulted from the first questionnaire was reviewed by the experts to check for misinterpretations. The answers from the narrowing-down and ranking questionnaires are analyzed statistically. I also used secondary data sources for validation and triangulation in the case studies.

"The process of interpretation moves from a precursory understanding of the parts to the whole and from a global understanding of the whole context back to an improved understanding of each part, i.e., the meanings of the words."

(Klein & Myers 1999, p.71)

5 Research Publications

To formulate and address the research questions raised in Chapter 1, I conducted the research approach described in Chapter 4. This resulted in five publications that are listed in Table 16. The full text of each publication is provided in the Appendix. Paper1 and Paper2 build on the literature; Paper1 describes the organizational field, the factors that influence CC adoption and the various adoption strategies within the frame of neo-institutional theory. In Paper2, I identified the research gaps in the existing literature. Paper3 builds on the case study of Egypt and Paper4 builds on the case study of Norway. Both Paper3 and Paper4 apply neo-institutional theory. Paper5 builds on the ranking-type Delphi study. Although the Delphi study started before the case studies, Paper5 could only be written after a long process of data collection, which took place between September 2013 and March 2015. The five publications are related to the research questions in Table 17.

Table 16: List of publications

Paper#	Reference
Paper1	El-Gazzar, R., & Wahid, F. (2013). An Analytical Framework to Understand the Adoption of Cloud Computing: An Institutional Theory Perspective. In *Proceedings of the International Conference on Cloud Security Management (ICCSM2013)* (pp. 91–98). Academic Conferences and Publishing International.
Paper2	El-Gazzar, R. F. (2014). A Literature Review on Cloud Computing Adoption Issues in Enterprises. In *IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014* (pp. 214–242). Springer Berlin Heidelberg.
Paper3	El-Gazzar, R. F. (2015). The Start of a Journey to The Cloud in The Developing World : A Case Study of Egypt. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS 2015)* (pp. 4345–4354).
Paper4	El-Gazzar, R. F., & Wahid, F. (2015). Strategies for Cloud Computing: Insights from the Norwegian Public Sector. In *Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2015)*.
Paper5	El-Gazzar, R. F., Hustad, E., & Olsen, D. H. (2016). Understanding Cloud Computing Adoption Issues: A Delphi Study Approach. (Accepted for publication in the Journal of Systems and Software). The article is currently in-press: http://www.sciencedirect.com/science/article/pii/S016412121630036X.

Table 17: Relationships between publications and research questions

Research questions	Publications
RQ: How can we understand the phenomenon of CC adoption within organizations?	1,2,3,4,5
SQ1: What are the institutional factors that affect CC adoption in organizations?	2,3,4,5
SQ2: How do institutional factors shape CC adoption strategies?	2,3,4,5

In the sections 5.1 to 5.5, I summarize the contribution of each individual publication. Then, in Section 5.6, I consolidate the foundations and contributions of all the publications.

5.1. Paper1: Defining External Pressures and CC Strategies

El-Gazzar, R., & Wahid, F. (2013). An Analytical Framework to Understand the Adoption of Cloud Computing: An Institutional Theory Perspective. In *Proceedings of the International Conference on Cloud Security Management (ICCSM2013)* (pp. 91–98). Academic Conferences and Publishing International.

Abstract

Although CC can offer potential benefits, CC still poses some serious concerns. Why do organizations adopt CC in spite of its potential risks? Based on several core concepts of institutional theory (DiMaggio & Powell 1983; Oliver 1991) and selective literature on CC, an analytical framework is proposed to better understand the adoption of CC by organizations. The focus was on the concepts of field-level changes, organizational fields, institutional isomorphism, and strategic responses within the context of CC adoption.

Findings

Based on the selective literature, I identified several organizations that form an organizational field and bring about changes (i.e., CC providers, peer organizations, business partners, professional and industry associations, and regulators). These may trigger institutional pressures (i.e., coercive, normative, and mimetic) on the adopting organizations. Furthermore, I also identified possible strategic responses (i.e., acquiescence, compromise, avoidance, defiance, and manipulation) to the institutional pressures related to CC adoption.

The framework, illustrated in Figure 13, was used for analyzing the findings from two cases; one from Egypt and one from Norway, which were published subsequently as Paper3 and Paper4. Furthermore, at a subsequent stage, some findings from the Delphi follow-up interviews were analyzed using this framework.

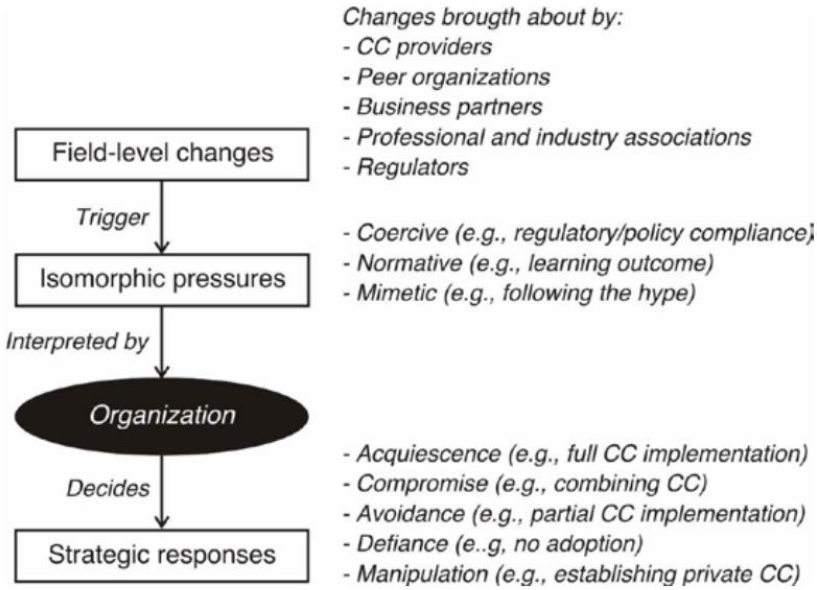


Figure 13: The analytical framework for understanding cloud computing adoption

5.2. Paper2: A Literature Review

El-Gazzar, R. F. (2014). A Literature Review on Cloud Computing Adoption Issues in Enterprises. In *IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014* (pp. 214–242). Springer Berlin Heidelberg.

Abstract

This paper explores the current key issues related to CC adoption through a systematic literature review. This is achieved by reviewing 51 published papers on CC adoption. This review used the grounded theory approach put forward by Wolfswinkel et al. (2011) and guidelines for conducting a systematic literature review presented by Okoli and Schabram (2010), and Webster and Watson (2002). The review covered all papers published up until February 2014.

The reviewed articles were classified into eight main categories: internal, external, evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation. Then, the eight categories were categorized into two

abstract categories: CC adoption factors and CC adoption processes, where the former affects the latter. The findings of the paper suggest that theoretical, methodological, and empirical contributions are needed to the area of CC adoption by enterprises.

Findings

The key findings from the review are discussed in Chapter 2 at the end of Section 2.4. The review implies the need for a cross-country analysis of the CC adoption phenomenon (e.g., developed vs. developing countries) (Greengard 2010). Methodologically, the review indicates the predominance of quantitative and conceptual studies over qualitative studies; surveys were mostly used among the reviewed studies, while field studies, case studies, and Delphi studies were relatively few in number. Accordingly, in this paper, I argue that Delphi studies are necessary in order to provide decision-makers with an insight into the most important issues, and the relative priorities, all of which should be considered when deciding to adopt CC services.

Various theories that have been used to study CC adoption were also reported in the review. However, I found no study in the reviewed articles that used institutional theory. This indicates the need for the widespread use of neo-institutional theory to explore the impact of institutional influences on the adoption of CC, particularly on how client organizations respond to those influences, and why organizations choose to adopt or do not adopt CC. The findings from my literature review correspond to reviews of empirical studies focusing on IS/IT outsourcing and CC, and there is a call for more in-depth examinations of institutional influences (Lacity et al. 2010; Schneider & Sunyaev 2014).

5.3. Paper3: Egypt Case Study

El-Gazzar, R. F. (2015). The Start of a Journey to The Cloud in The Developing World : A Case Study of Egypt. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS 2015)* (pp. 4345–4354). doi:10.1109/HICSS.2015.520

Abstract

This paper presents an exploratory case study in order to understand CC adoption factors and strategies in Egypt. The study is based on various data sources: 13 semi-structured interviews using different modes of communication, document and text

analysis, including official reports and news articles, and video recordings (details are provided in Chapter 4, Section 4.4.4). The interviews were conducted with various stakeholders. These stakeholders were chosen purposefully, and include CSPs that operate privately.

The study defined the field level changes in the Egyptian context. The findings of this study were analyzed by utilizing concepts from neo-institutional theory (i.e., isomorphic pressures and strategic responses to institutional processes) (DiMaggio & Powell 1983; Oliver 1991). According to the findings, factors that enable or inhibit CC adoption in Egypt are variously associated with CC per se, with limitations in developing countries in general, and the Egyptian context in particular.

Findings

The strategies chosen to adopt CC services are associated with the search for socio-economic development, and efficiency in doing business. On the other hand, non-adoption is associated with (1) vendor lock-in, (2) political uncertainty, which manifested itself as distrust that Internet cut enacted by the government during the revolution will not happen again. Such distrust can affect businesses, because CC is mainly dependent on the Internet, (3) limited connectivity, which is a common problem of the IT infrastructure in Egypt in terms of speed and stability, (4) data security, which results from the mental culture of 'having own data on own site' and a lack of a legal framework, because regulators are in place but regulations are not, (5) resistance to change, which can be clearly seen in long-established managers. Such resistance results from the fear of eliminating the role of CIOs, and (6) a lack of awareness about CC concepts, which are often seen to be the same as virtualization. Often, companies do not know how good or bad CC can be.

5.4. Paper4: Norway Case Study

El-Gazzar, R. F., & Wahid, F. (2015). Strategies for Cloud Computing: Insights from the Norwegian Public Sector. In *Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2015)*.

Abstract

This paper presents an exploratory case study to understand CC adoption factors and strategies in the Norwegian public sector. The study is based on various data sources: nine semi-structured interviews conducted through various communication modes, and

document analysis, including research articles, reports, and official documents generated by the Norwegian Data Protection Authority (Datatilsynet), the Norwegian government authority, and news articles (details are provided in Chapter 4, sub-section 4.4.4). Various stakeholders were interviewed, including cloud service providers, consultancy, and customer organizations from the public sector. The study defined the field level changes in the Norwegian context. The findings of this study were analyzed using concepts taken from neo-institutional theory (i.e., isomorphic pressures and strategic responses to institutional processes) (DiMaggio & Powell 1983; Oliver 1991). The study identified factors that either hinder or foster the adoption.

Findings

The findings indicate that the adoption of CC in the Norwegian public sector is driven by the search for efficiency and legal legitimacy. In this study, the desire for legitimacy manifested itself in the use of the standard agreement provided by Datatilsynet to procure public CC services, a thorough risk assessment, and negotiations with CSPs who adhere to Norwegian laws. The reasons for non-adoption include: unsolved complexity, organizational conflicts, and specific business needs. However, the risks associated with the CC model itself were not a factor. Furthermore, the study found that a certain strategic response could trigger an aggressive influence. This aggressive influence is a strong coercive influence that goes beyond enacting regulations (e.g., banning). It revealed that previous unlikely incidents reported in the media (e.g., the case of Narvik municipality) had influenced the Norwegian public organization's adoption strategy.

The complexity of the legacy solution appeared to be one of the key reasons for the avoidance of full CC adoption. This manifested in proofing concept of CC solutions to avoid complexity issues that may arise from the dependency of many system modules on public records. The desire to maintain a degree of internal competence to cope with rapidly changing business rules was seen as a reason to implement a private cloud. The fear of losing control over data secrecy was also a reason; here, non-adoption was influenced by the bureaucracy, conflict of interests, and goal ambiguity. Hence, non-adoption had no direct link with the risks associated with the adoption of the CC model itself.

5.5. Paper5: Delphi Study

El-Gazzar, R. F., Hustad, E., & Olsen, D. H. (submitted to a journal). Understanding

Cloud Computing Adoption Issues: A Delphi Study Approach. (under review)

Abstract

This paper presents the ranking-type Delphi study (Okoli & Pawlowski 2004; Schmidt 1997), which aimed to explore, identify, and rank the most important issues for adopting CC. The study began with 34 experts from different industries and public institutions. These experts took part in a Delphi panel, which was divided into three subpanels that represented different stakeholders (i.e., clients, providers, and academics). The study started in 2013 and was completed in March 2015. The Delphi study procedure comprised three stages: (1) brainstorming, (2) narrowing down, and (3) ranking. Follow-up interviews were also conducted with 16 experts to gain an in-depth understanding of the issues identified.

Findings

The panelists identified 55 issues of concern in the first round. These issues were analyzed and grouped into 10 categories: (1) security, (2) availability, (3) migration, (4) business, (5) legal and ethical concerns, (6) culture, (7) awareness, (8) impact, (9) strategy, and (10) IT governance. The top 18 issues of each subpanel were ranked and re-ranked, and the intrapanel agreement showed a low to moderate consensus on the issues. Security, strategy, and legal and ethical concerns were among the highest-ranked issues by all the subpanels. Follow-up interviews were also conducted to gain a deeper understanding of the topics revealed.

The results reflect different perspectives across the subpanels, especially for the clients and providers; the client subpanel ranked the issue "Data protection legislation is different and not strong in all countries" as number one. The provider subpanel ranked the issue "The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that in public clouds. However, risks are not absolute, and most of them can be addressed, but not all of them" as number one. The academic subpanel ranked the issue "Enterprises are faced with weak undetailed SLAs from providers (e.g., providers may not be transparent about where and how do they store the data, and the acknowledgement of security incidents whenever they happen and how the cloud provider deals with them)" as number one. The most important issues of concern were discussed in the paper.

It should be noted that, as the Delphi study was exploratory, I began by questioning the issues that confront enterprises when adopting CC services. By "issues", I mean

the important topics or problems that are raised in the debate about CC adoption in enterprises. However, as the data collection rounds progressed, and so did the analysis, these issues described the importance of some factors identified in this thesis and will be discussed in Chapter 6.

5.6. Bringing Together the Whole Story

The five presented publications convey the whole story of my thesis. The relationships between the five publications are illustrated in Figure 14.

To understand the CC adoption phenomenon, I systematically reviewed the IS research stream in this area and identified research gaps (cf. Paper2). This systematic review provided the theoretical, empirical, and methodological avenues for my research. It provided theoretical avenues that indicated the need to use neo-institutional theory to study CC adoption and gain a greater insight into the institutional factors that influence it and how client organizations respond to these factors. Paper2 also provided methodological avenues in terms of the need for more case studies and Delphi studies to provide a greater insight into knowledge and practice. The gap in previous empirical studies reviewed in Paper2 provided avenues for my empirical work.

Paper2 helped to identify a lack of studies that explore the external and internal institutional factors in different contexts (e.g., countries or sectors) in the context of CC adoption. This guided my choice of the empirical context of my study, including the formulation of research questions, and my selection of the theoretical lens and research methods. Furthermore, Paper1 conceptually developed the theoretical foundation, which enabled the later analysis of my field data.

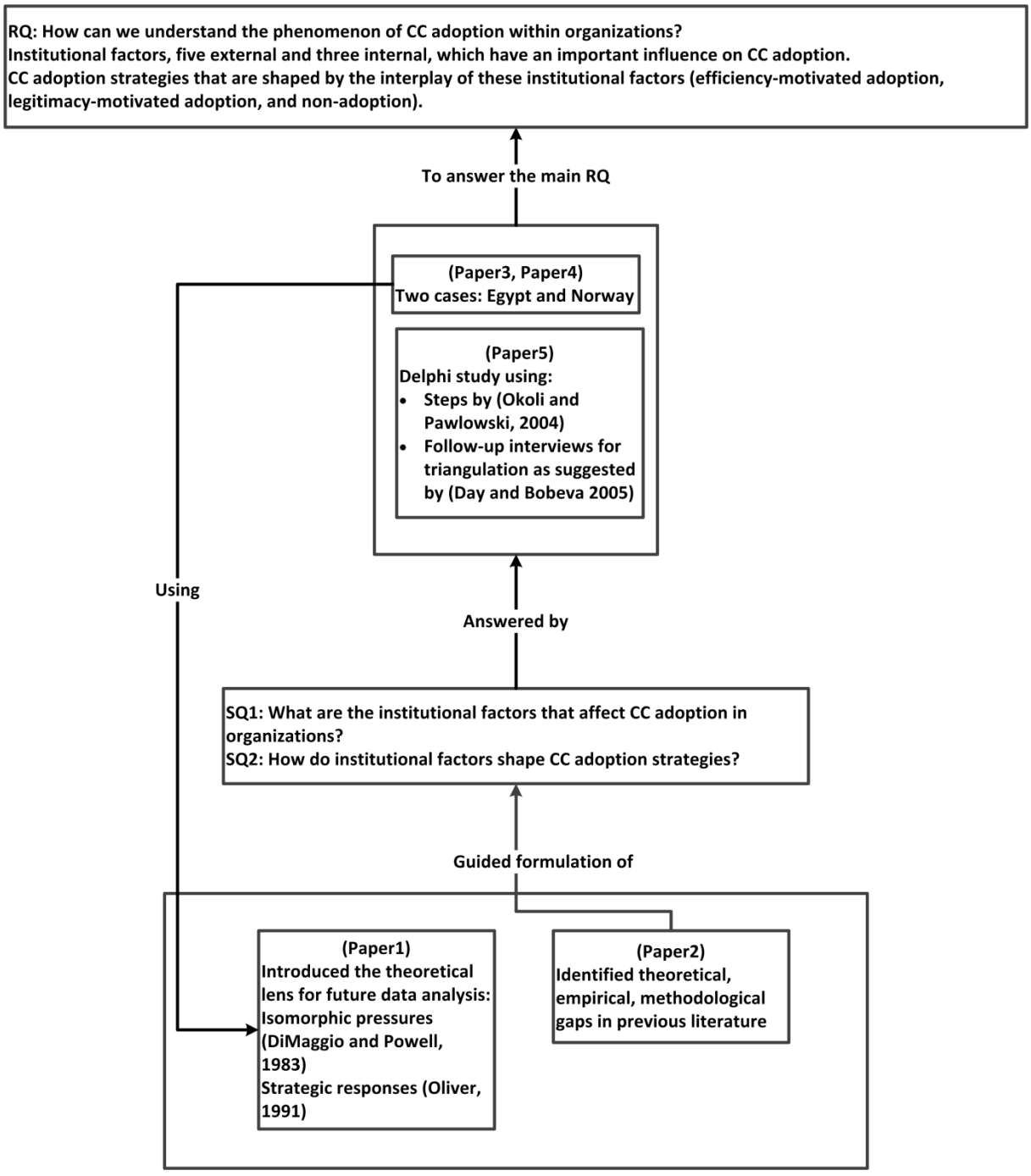


Figure 14: Relationships between publications

Paper1 is based on concepts taken from neo-institutional theory (i.e., field-level changes, isomorphic pressures, and strategic responses) and selective literature on CC. The theoretical foundation built in Paper1 was used for data analysis in Paper3 and Paper4. Empirical research gaps in the existing IS literature on CC adoption (cf. Paper2) guided my research focus on gaining a better understanding of the CC adoption phenomenon. Hence, SQ1 and SQ2 were formulated, and both the SQs were answered from the field by Paper3, Paper4, and Paper5. The empirical context for Paper3 was Egypt as a developing country, with a focus on CC initiatives and the

socio-political context. The empirical context for Paper4 was Norway as a developed country, with a focus on the public sector and legal context. Six countries from the public and private sectors, and of all sizes, formed the empirical context for Paper5.

Exploratory interpretive case studies, including interviews, video transcripts, and content analysis, formed the methodological foundation for Paper3 and Paper4. The analysis of the data collected from the two case studies was carried out using neo-institutional theory (i.e., field-level changes, isomorphic pressures, and strategic responses). In Paper5, a ranking-type Delphi method was used for data collection, involving brainstorming, a narrowing-down phase, two ranking rounds of questionnaires, and follow-up interviews. The analysis of data collected from the Delphi surveys was carried out through manual coding and non-parametric statistical tests. The data collected from the follow-up interviews served as explanations for the Delphi ranking results.

The findings from Paper3, Paper4, and Paper5 served to answer the main RQ by identifying the external and internal institutional factors that have an important influence on CC adoption strategies, together with the CC adoption strategies that are shaped by the interplay of these institutional factors. These strategies range from the efficiency-motivated adoption of CC, and legitimacy-motivated adoption of CC, to the non-adoption of CC, because of a lack of trust and an unclear vision. In the next chapter, I elaborate further on the contributions made by the five publications in answering the research questions posed in this thesis.

“The Black Swan asymmetry allows you to be confident about what is wrong, not about what you believe is right.”

― Nassim Nicolas Taleb

6 Discussion of Main Findings

In this chapter, I incorporate the main findings from the five research papers. In so doing, I discuss the main findings in light of the empirical data and in relation to the research questions. In Section 6.1 of this chapter, I present an overview of the findings that contributed to our understanding of the phenomenon of CC adoption in order to answer the main RQ. Thereafter, in Sections 6.2 and 6.3, answers to the two SQs are given through a detailed discussion of the institutional factors that were found to shape the CC adoption strategies.

6.1. Understanding The Adoption of CC Services

RQ: How can we understand the phenomenon of CC adoption within organizations?

To understand the CC adoption phenomenon, I systematically reviewed the research literature and identified research gaps (cf. Paper2). First, from the literature, I defined organizations that form the organizational field and bring about changes, including CC providers, peer organizations, business partners, professional and industry associations, and regulators that may trigger institutional pressures on the adopting organizations, and possible adoption strategies (cf. Paper1). Thereafter, I explored these institutional pressures and strategies through two case studies (cf. Paper3 and Paper4) and a Delphi study (cf. Paper5). The empirical material provided insights that supported my understanding of how current dynamics can shape the adoption of CC services.

It should be noted that Paper2 aimed to understand the existing research trends and to identify the research gap in order to formulate the research questions for this thesis. Although prior knowledge is important as a starting point for our understanding of a topic, it can cause bias that hinders discovering a new knowledge of reality that is socially constructed as interpretive researchers (Klein & Myers 1999). As an interpretive researcher, I relied on sensemaking to understand the empirical data as the situation emerged, rather than applying predefined variables from the literature (Klein & Myers 1999).

CC adoption phenomenon can be understood through external and internal institutional factors, which have an important influence on the choice of CC adoption strategies. Paper5 provided insights into the degree of importance of these factors through evidence gathered from the Delphi rankings. Second, the phenomenon can be

understood through the CC adoption strategies that are shaped by the interplay of these institutional factors. These strategies range from the efficiency-motivated adoption of CC, and legitimacy-motivated adoption of CC, to non-adoption, because of a lack of trust and an unclear vision. The identified institutional factors, the interplay between them, their influence, and the CC adoption strategies will be presented and explained subsequently. The findings will be discussed in light of the empirical data.

Based on the findings, CC adoption is enabled, constrained, inhibited, or confused by a set of external and internal institutional factors. The *external factors* are related to the external social environment, both locally and globally (i.e., governments and regulatory bodies, cloud providers, media, socio-political changes, and culture). The *internal factors* are related to the internal social and technical environment (i.e., internal stakeholders, firm characteristics, and IT infrastructure). The interplay between external and internal factors will be explained. The evidence from the data indicates that these factors have an influence on the choice of adoption strategies (i.e., efficiency-motivated adoption, legitimacy-motivated adoption, or non-adoption). Each strategy encompasses any of the adoption processes, including evaluation, proofing concept, decision, implementation, and integration. These processes have been identified in my systematic literature review (cf. Paper2).

Efficiency-motivated adoption involves a drive for efficiency brought by CC solutions to internal work practices without careful consideration of important external factors (e.g., regulations) or internal factors (e.g., IT infrastructure or processes, and routines). On the other hand, *legitimacy-motivated adoption* considers both external and internal factors for the sake of gaining legitimacy, while still increasing efficiency and improving on work practices. It should be noted that efficiency-motivated adoption is not a conscious choice that is driven by efficiency. Furthermore, it may also be confronted by alternatives that may create a strong coercive pressure that goes beyond enacting regulations (e.g., banning); this can lead to a legitimacy-motivated adoption that is more conscious and seeks legitimacy.

Non-adoption is when organizations ignore the idea of adopting CC services, even though the adoption was considered earlier. Reasons for non-adoption include a lack of trust and an unclear vision. Figure 10 summarizes the findings with regard to answering the main RQ. The upper part of Figure 10, which presents institutional factors, offers answers to SQ1. In Section 6.2, the answer to SQ1 is given; this

includes explanations for each institutional factor and its influence. The lower part of Figure 15 provides the answers to SQ2, which will be presented in Section 6.3.

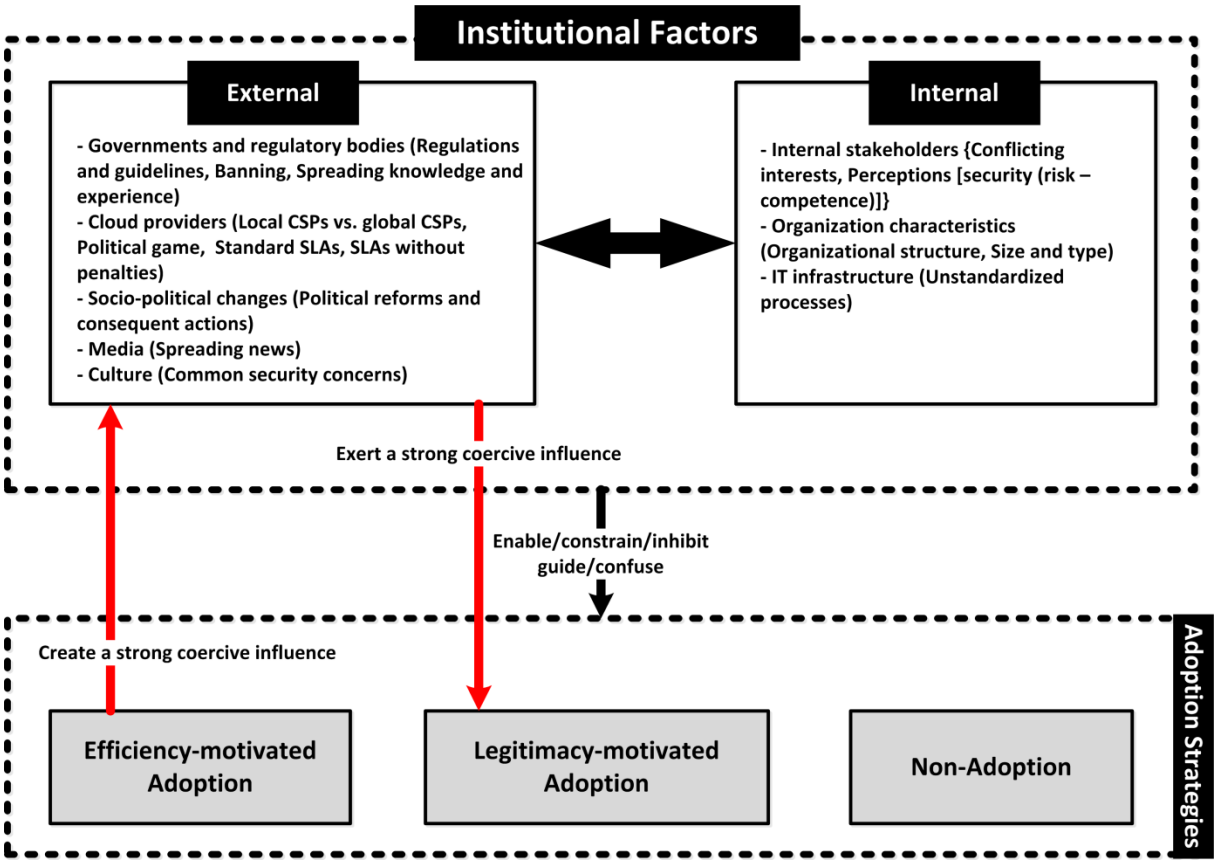


Figure 15: Understanding cloud computing adoption phenomenon

6.2. *Institutional Factors in the Context of CC Adoption*

SQ1: What are the institutional factors that affect CC adoption in organizations?

Addressing this SQ1 involved the identification of the institutional factors. Eight institutional factors were identified (See Figure 10 in Section 6.1). Five external factors were identified that are related to the external social environment, both locally and globally (i.e., governments and regulatory bodies, CSPs, media, socio-political changes, and culture). Three internal factors were identified that are related to the internal social and technical environment of the organization (i.e., internal stakeholders, firm characteristics, and the IT infrastructure). The external factors will be introduced in Section 6.2.1 and the internal factors in Section 6.2.2.

6.2.1. External Factors

Five external factors were identified that are related to the external social environment, both locally and globally (i.e., governments and regulatory bodies, CSPs, media, socio-political changes, and culture).

Governments and regulatory bodies: three governmental influences were evident (i.e., enacting regulations and guidelines, banning, and spreading knowledge and experience). Both the banning and enacted regulations and guidelines have been interpreted as coercive pressures from the case study of Norway. The influence of spreading knowledge has been interpreted as a normative pressure from the case study of Egypt. The final Delphi ranking results show a noticeable concern about regulations and compliance by the client subpanel (cf. Paper5). Regulations vary from one context to another and are not strong in all countries; this was ranked as number one issue by the client subpanel and as number three by the academic subpanel, according to the Delphi ranking results. Furthermore, the concern about compliance was a priority for both the client and provider subpanels. In countries where regulations are strong, compliance with such regulations is likely to slow down the adoption of CC services; this was ranked as number five by the client subpanel and number four by the academic subpanel. Furthermore, regulations are numerous and clients may not be able to get an overview of them. This was ranked as number five by the provider subpanel, because it can confuse clients and lead to the application of traditional regulatory compliance, which does not cover all CC aspects. Furthermore, these rankings remained the same during the first and second ranking rounds. This reflects the stable and equal views held by clients and CSPs on compliance, namely, that compliance inhibits, slows, and constrains the adoption of CC.

The ranking results regarding regulations are corroborated with the findings from the case study of Norway. The results demonstrate that regulations serve as an inhibiting and constraining factor (cf. Paper4). On the other hand, the laws in Egypt were not in place; this served as an inhibiting factor, because clients felt that their rights would not be protected if something went wrong with their data. This empirical finding has emerged from the empirical data and it has not been interpreted using predefined concepts from neo-institutional theory, though it was among the reasons for the defiance strategic response in the case study of Egypt (cf. Paper3). Government can have a rather strong coercive influence if the regulations regarding data location restrictions are violated, which can lead to banning, or inhibiting the adoption of CC services. This was the case for Narvik municipality, which was an early adopter of CC services in the Norwegian public sector. This municipality, which had an outdated IT

solution and lacked the required skills to maintain it, had a desire to move to CC services in order to benefit from more cost-effective mobile solutions (Jørgenrud 2011). Although they sent requests to IBM, Microsoft, and Google, they only received one reply, and that was from Google. In this case, the municipality faced a situation of limited alternatives, as not many CSPs were willing to reply to Narvik's request. Furthermore, they made a choice that was not conscious with regard to regulations; they entered into an agreement with Google for Google Apps without a clear statement about the location of the data. This caused the government to ban the use of Google Apps in the municipality until they were able to obtain such information. Consequently, Narvik municipality changed the agreement with Google and received information on the location of their data. The Norwegian Data Protection Authority (Datatilsynet) allowed Narvik to continue using Google Apps, but conditionally upon following certain guidelines (Datatilsynet 2012). The case of Narvik demonstrates an example of an efficiency-motivated adoption strategy; their choice was not conscious with regard to regulations. This choice created a strong coercive influence, which turned the adoption strategy into a legitimacy-motivated adoption after a ban was placed.

Narvik's case was a lesson learnt for the municipality itself and for other adopting municipalities afterwards, such as Moss, and two municipalities of clients C5 and C9. Moss requested guidelines from Datatilsynet before they started to use Microsoft Office 365 (Datatilsynet, 2012). Moss aimed to have a federated cloud-based e-mail platform to improve the quality of employees' work and to gain flexibility in users administration. In addition, the aim was to eliminate maintenance overhead of IT resources (Moss Kommune, 2013). Given the lesson learnt from the case of Narvik, Moss used Microsoft Office 365 for efficiency purposes; however, at the same time, they sought legitimacy by requesting guidelines from Datatilsynet to evaluate the agreement entered into with Microsoft for using Office 365 (Veum & Nymoen, 2012). Municipalities of clients C5 and C9 used the agreement enacted by Datatilsynet unquestioningly.

Norwegian public organizations have to follow the guidelines and regulations that are enacted by Datatilsynet throughout the adoption process, from assessing the potential risks to the data, and selecting the right CSPs, to choosing the right CC service model and location of the data, and using a special type of data processing agreement. Hence, the case study of Norway implies that governments have a constraining coercive

influence through regulations, which are used to guide the careful adoption of CC services.

In contrast with the Norway case, government influence in the case of Egypt was more enabling for the adoption of CC services. The Egyptian government distributed knowledge and expertise in collaboration with CSPs and consultants by means of talks and workshops at the Cairo ICT conference. In the opening session of the CC forum event at this conference, the new minister for CIT stated that the purpose of MCIT is, first, to attract foreign investment in order to create job opportunities for young people and, second, to stimulate the market and support companies that work in the ICT sector. In this regard, he elaborated on the benefits of CC, and how it would be discussed at the event, saying: *"There are various cloud computing business models, which will be discussed in detail, that offer competitive advantages for all users including large, small, and micro enterprises. This seminar will be followed by a number of workshops arranged under the auspices of MCIT and run by participating partners from national and international companies to understand the potential of cloud computing applications in the Egyptian market […] I hope that all parties including national and international companies, ministries' representatives, or other institutions in all sectors collaborate together to achieve fruitful outcomes from this forum. I expect that this will result in absorbing experiences from international companies and gaining maximum benefits."*

Although regulations are currently absent in the strategy for an Egyptian government cloud, there is a plan to establish a governance authority to regulate the adoption of CC services (MCIT 2014b). Nonetheless, I found no recent references on the progress of establishing this authority. CSPs view the notion of establishing governance authority and regulations to be a long process, which can inhibit innovation; indeed, this was mentioned by two representatives of CSPs at the Cairo ICT conference. The Egypt case implies the normative enabling influence of governments that advocate the wide adoption of CC services, as seen at the Cairo ICT conference.

Both the Egypt and Norway cases gave an insight into the need for regulations and the role of governments. The rankings also provided an insight into the important influences that governments can bring through regulations; these influences are inhibiting, constraining, and confusing. This sense of importance was felt strongly by the three Delphi subpanels. Additionally, the Delphi study revealed more influences resulted from regulations. Hence, the two methods (i.e., the case study and Delphi

study) achieved the purpose of triangulation. As a lesson to learn, the discrepancy between data protection regulations across countries needs to be resolved by having widely agreed governance laws and policies for exchanging data, which emulate those for exchanging money in the financial industry as provider P1 stated: *"the biggest problem is in policies and laws; cloud computing by its very nature is global! So in order to regulate cloud computing with respect to security and privacy, you need to have international agreement and laws and policies regarding data and privacy. It's very similar to the international governance that is in place in the finance community. Cloud computing service providers and banks are somewhat the same! In a bank, you give them your money […] CSPs; you give them your data. You trust the bank with your money….you trust the CSP with your data. […] It's governed finance but only for data related to money! Now you have to deal with data related to all sort of thing! There needs to be international norms set for cloud security; this doesn't exist yet!"*

Media: conclusions on this factor were drawn from the Delphi follow-up interviews and the Norwegian case study. Here, "media" denotes the spreading of news about previous cases and leaks either online or in print. This influence has been re-interpreted as a normative pressure guiding organizations to seek legitimacy when adopting CC services. The Narvik case was widespread in the news. As a result, other organizations went on to the legitimacy-motivated adoption of CC services. They did so by carefully adhering to Datatilsynet's guidelines in order to avoid appearing in the newspapers as was the fate of Narvik municipality, which was banned from using Google Apps (cf. Paper4). This implies the normative guiding influence of media towards the legitimacy-motivated adoption of CC services.

The "Snowden effect" was quoted by one client and three providers from the Delphi study and Norway case study (cf. Paper4 and Paper5). The role of the media in spreading this effect could cause an organization to stop dealing with a certain CSP, as was asserted by provider P13: *"We struggled with that […] we had the Snowden case for us stopped a big project to move all the business mailboxes in Norway 30000 mailboxes were supposed to be moved into Office 365 cloud, the project was stopped after all the news headlines with Edward Snowden said that the US is reading your mailboxes, if you move them to […] American companies, we have to stop it. So now we are moving the mailboxes to another data server in Norway instead; it is not more secure but the perception because of media made that necessary"*.

The influence of the media in spreading Snowden's leaks caused an on-going debate regarding global versus local CSPs. The Snowden effect led clients to prefer local storage with a compliant local CSP over that offered by more experienced global CSPs. On the other hand, CSPs do not always agree with clients' views, as will be explained in the following factor about cloud providers.

Cloud providers (CSPs):

CSPs' experience in CC industry and their compliance with regulations are related to the media, and global versus local CSPs. Global CSPs, which are mainly US-based, are very concerned about increasing their maturity in the cloud market, and have the sufficient experience to compete on securing their CC services according to the findings from the Delphi's follow-up interviews (cf. Paper5). However, the influence of the media, especially the Snowden case now means that global CSPs represent a risk for client organizations. Hence, local CSPs have come onto the scene, demonstrating their adherence to government regulations and this finding has been interpreted as a mimetic pressure from the case study of Norway (cf. Paper4). These local CSPs aim to persuade client organizations to adopt their CC services by offering the local storage of data and adherence to Norwegian laws. This kind of mimetic pressure is lacking in the literature (Schneider & Sunyaev 2014). However, this was evident in the interviews for the Delphi study and the case study of Norway (cf. Paper4 and Paper5).

Some clients believe that local CSPs offer a greater guarantee to store data within the same country (e.g., client C11). Such thinking can be flawed, because some CSPs may use third party CSPs to store the data. Provider P4 highlighted this as a major concern: *"This is a big misunderstanding because it's by default a guarantee that smaller local providers store information at the same place where they are located; they may use third party providers that store data wherever they want."*

Even if local CSPs do not use third party CSPs and they store data locally, they may still not be secure enough if they lack the competence and expertise in security held by global CSPs. This was asserted by provider P12: *"if in general you say I would trust a local CSP more than the global one, I would disagree to that! The global CSPs are the ones attracting the best security talent, the best developers, they have the best and more secure data centers, and they operate on multiple continents. So if the US [data centers] were to disappear, they still have a data center in Europe."* Providers P13 and P12, and client C13 were of the same opinion. They agreed that global CSPs are as

mature as their clients and they are more careful to provide CC services in an appropriate manner; C13 mentioned: *"I get more worried from local CSPs who are new in the market, but large international CSPs, […] they are dealing with mature customers who have large legal entities, that if there is flaw in the contract, they will hunt them down!"*

The different views held by clients and providers with regard to global CSPs versus local CSPs debate raise some interesting points. The clients' perspective prioritizes the legal compliance of local CSPs over the security expertise of global CSPs. This resulted from the interplay between the Snowden effect and global CSPs' expertise. The providers' perspective prioritizes the competitive security expertise of global CSPs; they argue that local CSPs do not have an equivalent level of expertise. Client C13 embraced the notion of dealing with global CSPs, because he had experience from both the client and provider sides. C13 highlighted the issue of co-responsibility if the USA government was to access data centers of global CSPs. He gave an example for a US-based global CSP that he worked for after working with a client organization: *"The trust center of this US-based international CSP will have to obey the USA government, but they will transparently involve the customer before providing any access for the USA government. As a customer, I have to make sure that a term like that is mentioned in the contract."*

A further interesting finding that emerged from the Delphi interviews is the game played between CSPs and traditional IT providers. The political game between pure-play CSPs and traditional IT providers is particularly confusing for client organizations. Traditional IT providers claim to offer their IT solutions as if they are cloud-like, even though they are not. Thus, traditional IT providers will talk negatively about pure CSPs and vice versa. Consequently, clients will be more confused and also pure CSPs will find it difficult to sell their CC services. Provider P4: "*The traditional vendors will talk negatively about cloud services because they want to sell their traditional solutions and the cloud vendors do it the other way! And as a customer in the middle, you will be confused because the messages are quite different from different types of vendors […] It's a kind of political game that they try to take market share from each other."* Despite this empirical finding became apparent through only one single quote, it raised an interesting insight that deserves further validation.

The political game mentioned by provider P4 during the Delphi follow-up interviews, is a result of his experience in dealing with clients and his observations of the market

dynamics. Clients in my sample have not reflected on the political game, or its effect. However, this input from the Delphi study added a new insight to my study that would not have been the case if I had only carried out the two case studies. Thus, triangulation is achieved by capturing different dimensions of the same phenomenon.

A further influence of CSPs, and rather a constraining one, is the SLA. CSPs offer standard SLAs that cannot be changed by small organizations. This issue was ranked as number seven by academics during the two ranking rounds (cf. Paper5). However, this influence was given a low priority by clients and providers, who ranked it 28 and 32, respectively, in the first ranking round. Furthermore, it was not among the top 18 issues for clients and providers in the second ranking round. One explanation for this is that the majority of clients in my sample are from the Norwegian public sector, whilst the rest are from large corporations. Furthermore, the case study of Norway offers an empirical insight into the fact that global CSPs know about the data processing agreement that Datatilsynet obliged public organizations to use when contracting CC services (cf. Paper4). Consequently, CSPs accept this agreement instead of their standard SLA. Hence, public organizations can have the power to change the standard SLA of global CSPs. The findings from the Delphi study and the Norway case offer an insight into the different dimensions of organizations (i.e., size and type) and the impact this has on their ability to modify SLAs.

SLAs for CC services are weak and do not cover all the details that clients need to know; this issue was ranked as number one by academics during the two ranking rounds. For clients and providers, this did not feature in the top 10 of the ranked lists for both ranking rounds. The Norway case offered an explanation when client C5 commented that the language of the SLA is *"written by lawyers to lawyers"*. Norwegian public organizations are required, by law, to have a clear sight on the SLA; thus, they acquire assistance from law firms to understand the SLA and align it with the legal requirements, as happened in client C9's municipality, Narvik, and Moss. Client C9 asserted that they hired an external law firm to assist them in the risk assessment and in the handling of the data processing agreement. Narvik and Moss hired the law firm Simonsen for the same purposes (Veum & Nymoen 2012; Veum & Thoreid 2012; Olsen 2015).

The Delphi follow-up interviews indicated that CSPs no longer state penalties in their SLAs. The reason for not working with traditional SLAs that include penalties is that CSPs have a lot of clients and would not be able to afford to pay penalties for each

client; indeed, this would cause them to go out of business. Such a situation can have a confusing influence on clients. For example, provider P12 said: *"So [CSPs] don't guarantee 99.9% uptime of the cloud […] and some penalties, they just say you have to trust us on this and our track record proves that we have extreme availability […] that is our SLA. So, yeah I do see that might be confusing, but it is more and more vendors are moving in that direction."*

Socio-political changes: this empirical finding has emerged from the empirical data and it has not been interpreted using predefined concepts from neo-institutional theory, though it was among the reasons for the defiance strategic response in the case study of Egypt. Political reforms and revolutions can cause uncertainty to the extent that they inhibit the adoption of CC services. This is what happened in the Egypt case, when an arbitrary decree from Mubarak's government issued on 28th of January, 2011, resulted in the shutting down of the Internet (cf. Paper3). Such a decree was intended to stop people communicating and planning gatherings. However, it had an unlikely impact on businesses, especially the CC market in Egypt. In particular, it had an inhibiting influence on client organizations, because they could not risk making their entire business dependent on the Internet by using CC services. At the same time, CSPs had their businesses downgraded as a result of this decree. CSPs need to protect their business, as was noted by consultant P21 and expressed by provider P18: *"recently Egypt faced an Internet outage due to the decree from the government which is not accepted and we must have a law that prevents governments from forcing Internet providers to cut Internet services, as this becomes a very weak spot for cloud services trend in Egypt, all companies are now afraid from facing similar situation that their dependence on CC will lead to outage and will impact their business."*

After this political event, the Egyptian government sought to encourage the adoption of CC services through such initiatives as the Cairo ICT conference. As stated earlier, this was intended to spread knowledge and experiences.

"Egypt is currently going through economic and political situations that may not seem to be favorable, but in fact, we can say that with every great challenge comes a greater opportunity […] people are afraid and they have the right to be afraid, but our duty towards Egypt is to turn all these fears into fruitful hard work […] and through ICT community, Egypt can face any challenges and attract investments."

(CEO of Trade Fairs International Company on behalf of the MCIT)

We can compare the impact of the Egyptian government on CC adoption when it shut down the Internet during this period of political reform with the impact of the Norwegian government when it banned Narvik from using Google Apps. Both incidents differ in terms of degree and consequences. The impact of the Egyptian government was indirect; the Internet was shut down for political purposes to stop the gathering of revolutionary crowds. The consequences have indirectly shaken the client organizations' trust in putting their business in the cloud. In the Norway case, however, the government impact was directly on Narvik, and had a close relation to the adoption of CC services. The consequences of the Norwegian government's actions were to directly increase the consciousness of the client organizations towards having a legally compliant data processing agreement and conducting risk analyses.

Culture: culture was found to be an inhibiting factor led to non-adoption in the case study of Egypt. This empirical finding has emerged from the empirical data and it has not been interpreted using predefined concepts from neo-institutional theory, though it was among the reasons for the defiance strategic response in the case study of Egypt. It is related to the reluctance to keep the data off-premise, even though data security is technically guaranteed in terms of data encryption (cf. Paper3). This is stressed by provider P23: *"the problem in Egypt is mainly cultural. People share same concerns about 'my data should be with me'; it is like our Egyptian saying 'I would carry my son on my shoulders, rather than leaving him somewhere and looking for him afterwards.', although we encrypt the data at rest and on transfer and put firewalls. Additionally, we sign an agreement, through which we guarantee security of the data."*

This national culture of reluctance is embedded in individuals who own or work for client organizations. This cultural factor, which needs to be addressed, was noted by the Egyptian government as being one of the expected challenges to CC adoption in Egypt for the coming years (MCIT 2014b).

6.2.2. Internal Factors

Three internal factors have been identified that are related to the internal social and technical environment of organizations (i.e., internal stakeholders, firm characteristics, and IT infrastructure).

Internal stakeholders: when internal stakeholders have conflicting interests regarding the adoption of CC services within an organization, these conflicts usually stem from

the different backgrounds of the stakeholders and their various needs. As a result, an organization may face the challenge of having an unclear vision and being unable to accommodate all stakeholders' needs. Thus, it becomes an inhibiting factor that can lead to the non-adoption of CC services. This was ranked as number seven by the providers (cf. Paper5); although they ranked it as number four in the first ranking round. Nonetheless, for providers, this factor remained among the top 10. In this regard, informant C13 (who used to work for a client organization, but currently works for a provider organization) asserted in the first Delphi survey: *"Each team/department/Organization adopting their own concept of a cloud […] It is without a doubt a nightmare for a CTO to not have a clear vision or control over his/her environment."*

However, this factor was not given high priority by clients and academics; indeed, it was ranked as 26th and 29th respectively in the first ranking round, and was not among the top 18 issues ranked by clients and academics in the second ranking round.

Nonetheless, there is evidence from the case study of Norway that conflict is a dominant reason for non-adoption. This empirical finding has emerged from the empirical data and it has not been interpreted using predefined concepts from neo-institutional theory, though it was among the reasons for the defiance strategic response. (cf. Paper4). In client C11's municipality, the idea of adopting CC services was ignored, even though the idea was raised and discussed at a small conference held there. As client C11 has stated, the reasons for not choosing the correct strategy for using CC services in this municipality were threefold: (1) loss of control (concerns regarding data sensitivity and data location; (2) conflicts (small municipalities have different interests and knowledge about the use of IT compared with larger municipalities; and (3) bureaucracy (the multi-leveled structure of each municipality makes it slow to reach an agreement on any proposed strategy, especially as the gains are not yet clear to them).

Although client C11 saw security as the primary reason for not reaching a clear CC adoption strategy, he gave other reasons for non-adoption; among these reasons was the challenge to accommodate the conflicting interests of internal stakeholders. Such conflicting interests are one influence that internal stakeholders have on the adoption of CC services.

The second influence is the perceptions of stakeholders regarding data security risks (e.g., confidentiality). In the Snowden case, these risks resulted from an external factor

"the media", which publicized Snowden's leaks about the NSA and US government. This implies that clients require more security guarantees than those offered by CSPs; indeed, this issue was ranked as number two by clients during the two ranking rounds (cf. Paper5), while providers ranked it as number 17 in both rounds and academic gave it a slightly higher priority, changing their ranking from 11 to nine.

Thus, clients perceive security in the cloud as a risk that can result from dealing with global US-based CSPs, despite the fact that these CSPs are experienced in securing their solutions. On the other hand, CSPs assert that security in the cloud is better than in-house security and that they, as global CSPs, consider it a competence on which competition between CSPs is based. In this regard, provider P12 asserted: *"There is some sort of […] irrational fear. Why I call it irrational is that local data security is seldom more secure than having data stored with the best security providers in the world."*

Provider P7 asserted that clients often feel they have full control over their IT department and security issues. However, in her view, this is not true; rather, clients' local IT departments do not have the necessary skills to cope with security issues: *"the local IT departments do not have skills with regard to security to be able to protect the company as good! So it might be better to look to a vendor that is really skilled on this."*

Hence, CSPs are aware of clients' perceptions of CC risks and can make sure that they are offered a secure CC solution such as a private cloud; this issue was ranked as number one by providers, number two by academics, and number three by clients in both ranking rounds (cf. Paper5). Furthermore, in the Delphi follow-up interviews, CSPs' interpretations (P12, P4, and P6) highlighted that the risks posed by CC solutions are "not absolute" and need to be evaluated against the risks of other IT solutions. Even if risks exist, there are ways to mitigate them, such as certifications. As provider P6 asserted: *"if you are focusing very much on risk, then it could be a very negative outcome! If you decide not to go for a solution because it's too risky, then you turn around and go to another solution […] but then that solution also has a risk! […] Security issues can be mitigated by having certifications in place."*

Organization characteristics: this factor includes organizational structure and size, both of which have an influence on the adoption of CC services within an organization. The multi-leveled organizational structure has an inhibiting influence on the adoption of CC services, as was manifested in the Norway case where one of the

reasons that client C11's municipality did not achieve a CC adoption strategy was the multi-leveled bureaucratic structure (cf. Paper4). Such a structure makes it complicated to adopt CC services and slows down the process. This empirical finding has emerged from the empirical data and it has not been interpreted using predefined concepts from neo-institutional theory, though it was among the reasons for the defiance strategic response in the case study of Norway.

Informant C13 highlighted this notion of complex organizational structures in his response to the first Delphi survey; from his experience in a private worldwide client organization, he asserted: *"Transforming a traditional organization and restructuring it is essential for a clearer decision making process […] A shift in responsibilities may occur to adapt to the new model […] Sticking to an old organizational chart will lead to gaps in understanding new requirements/demands from all involved teams [and] elongating the decision making process."*

An organization's size (i.e., small or large) and type (i.e., public or private) also have a constraining or enabling influence on the power to change the SLA; this was found in both the Norway case and the Delphi study. The findings from the Delphi study indicated that it is hard for small client organizations to modify the standard agreements of global CSPs; this issue was ranked as number seven by the academic subpanel, as mentioned earlier. The case study of Norway provided an empirical insight, which was not theory-driven. Public organizations could have the power to replace the standard agreements of global CSPs with the data processing agreement set by Datatilsynet, especially as they cannot use CC services without this agreement (cf. Paper4).

IT infrastructure: an important aspect that comes into play is the standardization of processes. This corroborates with client C1's opinion stated in the Delphi follow-up interview: *"The problem is in the maturity of the organization itself […] the maturity of the processes because one of the basic requirements in the cloud is the 'standardization of processes'. I believe that an organization should go for cloud services based on its maturity rather than going for an upstairs technology just like that! Because of the inflexibility of cloud environments or cloud service providers and the low maturity level of the companies like us, it becomes a 'mismatch' in terms of effective utilization of cloud services."*

Complex unstandardized processes inhibit the adoption of CC services, leading to a mismatch, as client C1 has stated. Furthermore, these constraints can delay adoption,

because many workarounds have to be carried out. In C1's experience in a particular client organization, there were problems in integrating public CC solutions, because of existing legacy systems (cf. Paper5). Client C1 asserted that their adoption was driven by agility, but they realized that their processes were not standardized or mature enough for CC. Although their platform was never outdated, and all necessary upgrades were carried out, during the integration they still faced restrictions with the cloud solutions. In the end, adapters had to be developed for their legacy environment. Client C1 explained: *"The underlying fundamental reason was a strategic drive towards outsourcing and making the internal organization leaner, but in that entire process we missed out on 'whether we are ready for the cloud or not?!' a cloud service becomes much more effective in a matured standardized organization, which has more standardization across its functions […], but for a company like us, which is not that much standardized or is not in that kind of maturity it is a challenge."*

In C1's organization, they did not realize a priori and prepare for the challenge they would face when integrating CC solutions into their legacy systems. They were not prepared for the integration challenges and did not consider redesigning their current architecture. This can be attributed to the fact that clients usually invest in cloud services as a local initiative and not as a part of a business or IT strategy. As provider P4 asserted: *"I think typical sales and marketing, they go directly and buy, for example, Salesforce without involving IT staff in a good way – because IT staff will delay them and just ask questions that takes a lot of time to answer."*

Standardization is a significant factor that relates to the maturity of the clients' business processes and enterprise architecture. A number of experts in the Delphi study stressed that clients need a certain maturity in their enterprise architecture in order to be able to integrate CC services into the business in an appropriate manner. Provider P4 asserted: *"I think the most important [issue] is to understand the architecture and [. . .] if you have a good modular architecture, you can easily see if there are functionalities that [can be put in the cloud] and also if it has a very strong dependency on other systems, then you should not pick that one at the first phase."*

A number of experts also asserted that very few client organizations are presently at the required maturity level. A number of panelists also pointed out that redesigning the business model is key to reaping the benefits from CC services. The comment from provider P1 illustrates this: *"The real capability of the cloud is in redesigning the business model – and most of the people want to start with technology. And if you have*

that view, you don't change the business model, then you can't reap the broad benefits of transitioning to the cloud."

Client C2 made similar comments to client C1 and provider P4 about standardization; they faced the situation that PaaS offerings are standardized and very app specific. This was felt to be a constraint that would increase their dependency on the CSP. The case of client C2 implies a greater awareness of the current CC offerings and the existing IT infrastructure; hence, their decision to implement a private PaaS model was seen to be better than carrying out a manual adaptation of their existing infrastructure, as happened in the case of client C1.

To conclude, the extent of the challenge of adopting CC services relates to the maturity of the client's enterprise architecture and processes. Most client organizations lack the required level of maturity to integrate their unstandardized processes with standard CC services; thus, understanding and redesigning those processes prior to integration is key to realizing the benefits of CC. The identified institutional factors (i.e., external and internal) and their various influences are discussed with regard to the empirical findings in Sections 6.1.1 and 6.1.2. Combinations of these factors contributed with outcomes that shaped CC adoption strategies.

6.3. Institutional Factors and CC Adoption Strategies

SQ2: How do institutional factors shape CC adoption strategies?

The three CC adoption strategies are discussed in light of the empirical data in the subsequent paragraphs.

Efficiency-motivated adoption: as mentioned in Section 6.1, efficiency-motivated adoption is driven by efficiency, without careful consideration of important external factors (e.g., regulations) or internal factors (e.g., IT infrastructure, or processes and routines). This was evident in two stories: Narvik municipality and their acquiescence strategic response from the case study of Norway (cf. Paper4) and client C1's organization from the Delphi's follow-up interviews (cf. Paper5). Both of them were early adopters and did not consider important institutional factors. Narvik did not consider getting information about the location of the data, in accordance with Norwegian law. This is an external factor. However, after the ban, they changed the agreement and got information on data location.

In the case of client C1, they did not consider a priori the challenge that they would face when integrating their unstandardized legacy environment with public cloud solutions. This is an internal factor. Furthermore, they did not realize the level of restrictions in the CC offering as a result. Consequently, they cannot do much in the cloud environment. However, after much hard work on their legacy environment, they eventually managed to successfully launch a CC model. Perhaps client C1's organization would have needed to understand a priori the impact of integrating CC solutions to their legacy systems. This relates to the management of the migration to CC as asserted by client C5: *"So managing the migration, understanding the impact on us, and changing the way we do business on the way to the cloud, that is what I say is important."*

Legitimacy-motivated adoption: is driven by legitimacy, while still increasing efficiency and improving work practices. This was found applicable for late adopters, such as clients C4, C2, and C3 (cf. Paper4). In the case study of Norway, there was evidence from the compromise and avoidance strategic responses by the client C4's organization, the adoption strategy was in place, but the transition had not yet begun. They were at the stage of accommodating various institutional factors for the sake of legitimacy in the legal environment. They were aiming at sourcing IaaS and PaaS to the cloud, but their concern was the selection of the right CSPs to meet the legal requirements regarding data location. Furthermore, they were considering a criterion of high availability in their to-be architecture to guarantee a smooth transition without disturbing the current processes, which will determine the right CSPs for them as well. Additionally, a concept of mobile solutions was being trialled, with storage in the cloud, and they were evaluating how they could use CC services to establish a regional electronic public record that was both centralized and standardized. They are currently in the evaluation stage, because they recognize the challenge raised by the dependency of many systems on this public record.

In the case study of Norway, there was further evidence from the manipulation strategic response by the organization that C2 and C3 work for; various internal and external institutional factors have shaped their adoption strategy. After evaluating solutions that are available in the market such as Cloud Foundry; they did not find enough references for this solution in Norway (cf. Paper4). Furthermore, they were developing apps of a special type. Thus, having them deployed by available PaaS solutions would require them to do potentially cumbersome manual modifications. Thus, they decided to implement their own PaaS, as asserted by client C3: *"We have*

looked at some commodity implementations of PaaS […] we have found those products to be a bit immature […] Not very wide-spread in the market, no real resources with experiences locally in Norway at least. The current PaaS implementations are very App-specific. Ok I can deploy one App, but I have 50 [Apps]. That is not going to help that much, so we actually need either to script or automate against the [current] PaaS implementation. We are implementing now both an infrastructure as a service layer and on top of that PaaS."

In addition, this organization preferred to have internal IT competence, so that they could test their apps thoroughly, without having to wait for the CSP to fix any inconvenient errors that may occur. This would avoid any media attention if errors were not dealt with. Client C2 mentioned: *"The rules change every year in the [domain we operate in], so it is not a stable system. Testing is very important, because we have an issue with reputation. [then client C3 contended:] If there is a bug in the system and when we have sent it, it is too late to fix the system. It goes externally and in the worst case on the front page of the newspapers. So, we can't risk it. So, we need to test very thoroughly. That is an important goal of cloud strategy or automation strategy"*

It should be noted that the research findings indicate that efficiency-motivated adoption is not a conscious choice and driven by efficiency can create a strong coercive influence. This leads to legitimacy-motivated adoption, which is more conscious and is aimed at gaining legitimacy through a careful consideration of legal guidelines (cf. Paper4).

Furthermore, in the case of Egypt, the strategy of implementing an Egyptian government cloud was driven by the desire for legitimacy in the global market (cf. Paper3). External factors shaped this strategy (MCIT 2014b), including the normative enabling role of the government in collaboration with CSPs and consultants (cf. Paper3).

Non-adoption: involves ignoring the idea of adopting CC services, even thought they were considered earlier, either because of an unclear vision, or because of a lack of trust. It should be noted that the factors that shape non-adoption are not CC technology-related factors such as data encryption in the cloud; mostly, the factors are related to the external and internal environments. In the case study of Norway, there was evidence from the defiance strategic response of client C11's organization; the factors that contributed to non-adoption were internal (cf. Paper4). These factors took

the form of conflicting interests among stakeholders and the bureaucratic organizational structure, which contributed to the lack of clear vision towards adopting CC services. Thus, business cases are important to accommodate the different interests of various internal stakeholders as C13 asserted (a former client and a current provider):

"This is the most difficult part, to convince the senior management that this is the best solution for them and it will save money in the long term! That wasn't an easy task! Business cases have to be well-presented to overcome any political discussions and put the stakeholders in the right position before taking a decision."

Such business cases have to be focused on business needs rather than IT costs, and gradual actions of change need to be considered in order to avert reluctance towards CC adoption as Provider P4 emphasized:

"If you start with IT cost perspective, I think you will immediately have all the IT employees against you because when you are discussing change from internal operation to using cloud services, you are in the same time saying that some of you will be out […] you cannot tell a person just change a daily task in one day to another, you need to involve the people and let them also have a big impact on how their new roles will be. So I think it is quite dangerous to start with cost perspective and with the IT focus. So it is very important that you [are] focusing on business needs, and you need to defend that, if it is a high cost, it is for a lower operational cost, improved processes, or new services to the market, etc."

In the case study of Egypt, the defiance strategic response was influenced by several reasons related to external factors, such as a lack of legal framework, cultural concerns about security, and socio-political changes and their consequences, all of which contributed to a lack of trust that led to non-adoption (cf. Paper3).

"Cloud technology will become a game changer; however, it is a young phenomenon, and it is suffering from teething pains typical of its age. It's also subject to many overblown hype in the marketplace. Although the upside of cloud computing is big, numerous challenges lie ahead."

(Client C12)

7 Contributions

The objective of this thesis is to contribute to our understanding of the phenomenon of CC adoption. In this study, institutional factors were identified, along with the way they influenced the shaping of CC adoption strategies. Concepts from neo-institutional theory were applied to explain some of those institutional factors and adoption strategies. This thesis addressed the main RQ by exploring two SQs. Altogether, the answers given serve to explain the important influence that institutional factors have on CC adoption within organizations. Additionally, the thesis offers both theoretical and practical implications based on the empirical findings. The theoretical implications are discussed with respect to the existing assumptions in the literature. The practical implications offered include the CC adoption issues identified from the Delphi study that are important for decision-makers to take into account when considering CC investments. Furthermore, implications for CSPs and law-makers are offered as well.

7.1. Contributions to Knowledge and Theoretical Implications

After discussing the empirical findings, it is important to *"pay attention to a good upbeat ending"* by emphasizing the claimed contributions in terms of *"How do they advance our knowledge of the research topic? How do they extend the existing literature? To what extent are […] results generalizable to other contexts?"* (Walsham 2006, p.327). This thesis contributes to the CC adoption area by utilizing the neo-institutional theory to understand the CC adoption phenomenon. The contributions to CC adoption add insights into the empirical phenomenon of CC adoption; hence, they can be counted as empirical contributions that offer theoretical and practical implications. An empirical contribution is defined as *"a novel account of an empirical phenomenon that challenges existing assumptions about the world or reveals something previously undocumented"* (Ågerfalk 2014, p.594). The contribution to neo-institutional theory is that it is applied in new contexts of two case studies (i.e., CC adoption as a previously unexplored phenomenon using neo-institutional theory in Egypt and Norway), which offered empirical insights that provide theoretical implications (Harlow 2010). Table 18 summarizes the contributions in relation to the research questions. The contributions are further discussed against the previous literature and the neo-institutional theory in the subsequent sub-sections. Theory and empirical findings often go *"hand in hand"*; theory helps to *"organize our thoughts"* and *"explain phenomena"*, while empirical findings enable validating theory (Ågerfalk 2014, p.594).

Table 18: Summary of the contributions

Contributions	Description	Research Questions
CC adoption	The study has identified a set of institutional factors that affect CC adoption in organizations: -External factors related to the external social environment both local and global (i.e., governments and regulatory bodies, cloud providers, media, socio-political changes, culture). -Internal factors related to the internal social and technical environment (i.e., internal stakeholders, firm characteristics, and IT infrastructure).	RQ, SQ1
	The study has identified three CC adoption strategies along with the dominant reasons behind them: -Efficiency-motivated adoption that is driven by efficiency that CC solutions can bring to internal work practices without a careful consideration of important external factors (e.g., regulations) or internal factors (e.g., IT infrastructure or processes and routines). -Legitimacy-motivated adoption that is driven by gaining legitimacy through considering both external and internal factors for the sake of gaining legitimacy while still increasing efficiency and improving work practices. -Non-adoption involves ignoring the idea of adopting CC services, despite it was considered earlier, for having lack of trust and unclear vision that several institutional factors contribute to them.	RQ, SQ2
Neo-institutional theory	This theoretical lens was applied to understand the CC adoption phenomenon in a new context (i.e., Egypt and Norway) which is a different context from where the theory was originally applied; hence, this is counted as a contribution to theory. By utilizing this lens, a richer and broader understanding of the CC adoption phenomenon was achieved.	RQ, SQ1, SQ2

However, it has been claimed that a *"one-sided focus on theory"* and theoretical contributions may lead to an *"unhealthy behavior"* in terms of force-fitting the data into the theory and excluding *"truly exciting"* findings that contradict the theory, but offer significant theoretical implications and help seeing things differently (Ågerfalk

2014, pp.594–595). Thus, it should be noted that some empirical findings in this thesis have been explained in the individual cases studies (i.e., Egypt and Norway), and have been re-interpreted at a later stage of data analysis in combination with the empirical findings from the Delphi study, then, compared with the existing literature. Hence, some interesting empirical findings emerged and are included in the contributions of the thesis.

7.1.1. CC Adoption

In the following, the empirical contributions are discussed against the existing knowledge in the literature.

External Factors

Governments and regulatory bodies: The case of Narvik municipality demonstrates an example of an efficiency-motivated adoption strategy; their choice was not conscious with regard to regulations. This choice created a strong coercive influence, which turned Narvik's adoption strategy into a legitimacy-motivated adoption after a ban was placed. The literature has not yet reported on such a strong coercive influence of the government (Schneider & Sunyaev 2014).

The case study of Norway implies that governments have a constraining coercive influence through regulations, which are used to guide the legitimacy-motivated adoption of CC services after Narvik's case. Existing research has reported on the constraining influence of the government on the banking industry in the context of CC (Schneider & Sunyaev 2014). Only one study in the context of healthcare has reported the positive influence of government policy on the adoption of CC (Lian et al. 2014). However, the existing literature reported no evidence on how a lack of regulations can inhibit CC adoption, or on how the abundance of regulations can lead to confusion (Schneider & Sunyaev 2014).

In contrast with the case study of Norway, government influence in the case study of Egypt was more normative for enabling the adoption of CC services. The literature has frequently reported on the inhibiting coercive influence of governments (Schneider & Sunyaev 2014; DiMaggio & Powell 1983), although this may not be the case in other contexts. Indeed, in the case study of Egypt, the government role was more normative involving education and the exchange of experiences. As the context differs, the influence of the same factor differs as well (i.e., coercive and normative). This offers theoretical implications for further validation in the future.

Media: The literature reported that the influence of the media was mimetic, which contributed to the diffusion of IS/IT outsourcing practices (Hu et al. 1997; Schneider & Sunyaev 2014). When looking back to the 1980s and the rise of minicomputers, many organizations backsourced their IS functions that they used to outsource to external suppliers (Hirschheim et al. 2007). However, the announcement of Eastman Kodak's major outsourcing decision in 1989, once again brought about an increased tendency towards IS/IT outsourcing, known as the "Kodak effect" (Loh & Venkatraman 1992b). In the IS/IT outsourcing literature, it was reported as a source of mimetic influence on IS/IT outsourcing decisions (Lacity et al. 2010). What is happening now in the cloud market is that we see more turbulence and uncertainty, which slows down the adoption of CC services (e.g., Edward Snowden's leaks in 2013).

The literature tends to see the leaks about the PRISM program as related to the existence of the Patriot Act; the issue is, thus, related to the US legislation (Schneider & Sunyaev 2014; Cloud Security Alliance 2013). However, in my view, Snowden's leaks can be related to the media; if the media had not spread these leaks, organizations would not have known that the US government had access to their data, and they would not have been skeptical about dealing with US-based CSPs.

The role of the media in spreading Snowden's leaks has made many organizations more conscious about selecting the right CSP and making sure that their data is stored in a safe location, away from US surveillance. It represented a normative influence guiding towards a legitimacy-motivated adoption of CC service. Such leaks have caused considerable after-shocks in the cloud market; indeed, it is reported that 88% (from a total of 1,000) of decision-makers changed their buying behavior towards CC services as a consequence (NTT Communications 2014). It is also reported that in the EU region, 97% of decision-makers started to prefer buying CC services that are located within their own region (NTT Communications 2014). Spreading Narvik municipality's case in the news had also a normative influence. Having different influences based on the same institutional factor (i.e., mimetic and normative), offers theoretical implications for further validation in the future.

Cloud providers (CSPs): CSPs can influence CC adoption by sharing success stories with their clients, which has been reported in the literature (cf. Paper2). Furthermore, the literature has reported on the CSPs' compliance with regulations issues, their

assistance in migration, and their experience in managing the needs and concerns of client organizations in a responsible manner (cf. Paper2).

To the best of our knowledge, the debate on local CSPs versus global CSPs, that was evident in the empirical findings, is not reflected in the previous literature. Global CSPs are mature and experienced in the cloud market, and they compete on securing their CC services. This experience, according to the literature, has an influence on the reputation of CSPs (cf. Paper2). However, with the influence of the media (i.e., Snowden case), global CSPs represent a risk for client organizations. Hence, local CSPs aim to persuade client organizations to adopt their CC services by offering the local storage of data and adherence to Norwegian laws in the case study of Norway. This kind of mimetic influence by local CSPs is lacking in the literature (Schneider & Sunyaev 2014). It can be noted that the mimetic influence of local CSPs and normative influence of the media stand against global CSPs. This offers theoretical implications for further validation of the influence of multiple institutional factors.

The political game between CSPs and traditional IT providers was found to cause confusion for the clients, as the traditional IT providers talk negatively about CSPs, especially regarding security that is a critical issue in CC services, which discourages clients from adopting CC services. It should be noted that the literature lacks evidence on the similar influence of CSPs and traditional IT providers on the social aspect of security in CC adoption (Schneider & Sunyaev 2014; Su 2011; Saya et al. 2010).

The standard SLA of CSPs cannot be changed by small organizations, but public organizations can change it. Relating the size and type of organizations to their ability to modify SLAs, has not yet been discussed in the IS literature on CC and IS/IT outsourcing literature (Schneider & Sunyaev 2014). The literature had mainly reported on the likelihood of small organizations to adopt CC services than larger ones (cf. Paper2).

SLAs for CC services are weak and do not cover all the details that clients need to know. This finding is in line with the literature that reported on the transparency issues associated with SLAs and the need for parallel governance procedures (Morin et al. 2012; Schneider & Sunyaev 2014).

The literature also reported that SLAs for CC services are subject to small penalties in the case of inconvenient service unavailability (Lango 2014; Susarla & Barua 2011). However, the Delphi follow-up interviews indicated that CSPs no longer state

penalties in their SLAs, as they cannot afford to pay penalties for each client. This interesting empirical observation provides insights into new SLA issues that have emerged with CC, and did not exist in previous IS/IT outsourcing practices. The previous IS/IT outsourcing literature reported that in previous IS/IT outsourcing practices, agreements used to have penalties for non-performance (Susarla & Barua 2011; Lacity & Willcocks 1998). The IS/IT outsourcing literature encouraged the identification of changes in IS/IT outsourcing practices that are caused by emerging IS/IT outsourcing models, such as the CC model (Lacity et al. 2010). Although this empirical finding was not theory-driven, it is theoretically interesting (Ågerfalk 2014); it offers an empirical insights that imply the need for further development of endogenous theories, as it seems that new issues arise with the emergence of new IS/IT outsourcing models, such as the CC model, which would be more complex to explain by a single theory (Lacity et al. 2011; Schneider & Sunyaev 2014).

Socio-political changes: The Egyptian government's decree to shut down Internet providers had an unfavorable influence on client organizations' opinions when deciding to use CC services. Rather than seeing it as an opportunity; they perceived it as a threat to their business. Whilst the literature reported on the use of social networking sites, which are applications of CC, and are powerful tools in political reforms (Sultan 2013), no evidence was reported on the influence of such political reforms (e.g., the Egyptian revolution in 2011), or on the consequent actions that are taken during them (e.g., the government decree to shut down the Internet).

Culture: The cultural reluctance is embedded in individuals who own or work for client organizations, and represents an inhibiting factor for the adoption of CC services. This reluctance by individuals stems from the culture of the society itself as a country (i.e., Egypt in this case). A discussion of this factor is lacking in the CC literature (Schneider & Sunyaev 2014), even though the IS/IT outsourcing literature reported on the fact that IS/IT outsourcing decisions are culturally sensitive (Dibbern et al. 2012). Furthermore, the Egyptian context has been less explored in terms of institutional factors in the context of IS/IT outsourcing (Lacity et al. 2010) and CC. Existing research in the area of CC in the Egyptian context is limited; any that does exist has a quantitative and conceptual design focus. Indeed, only one study has been based on a survey, and has focused on education and assessing the effectiveness of using an open source Moodle e-learning platform to improve the quality of students' comprehension (Abou El-Seoud et al. 2013). Two studies have focused on proposing CC models for e-government. Of these, one study proposed a "Before Cloud E-

government" model for the transition of Egyptian e-government to CC (Nasr & Galal-edeen 2012). The second study proposed a hybrid model for e-government in Egypt to minimize security, privacy, reliability, performance, and legal concerns (Hana 2013).

Internal Factors

Internal stakeholders: The literature highlighted a gap in our knowledge about issues regarding internal stakeholders, such as conflicts (Schneider & Sunyaev 2014). The literature also reported on a rich list of CC benefits and security risks, together with certifications to mitigate risks (Schneider & Sunyaev 2014; Lansing et al. 2013; Venters & Whitley 2012; Morgan & Conboy 2013). However, the literature lacks detailed descriptions of the different perceptions of CC security (e.g., risk vs. competence) (Schneider & Sunyaev 2014).

Organization characteristics: The literature reported a noticeable lack of empirical evidence about restructuring the complex organizational structure of an organization in the context of CC (Schneider & Sunyaev 2014), despite the literature emphasized that the bureaucratic organizational structures may slow the adoption of CC (Seddon & Currie 2013). The importance of this factor was evident in the findings from both the Norway case and the Delphi study. Some existing studies have investigated the effect of firm size on the tendency of organizations to adopt CC services (Schneider & Sunyaev 2014). However, the literature lacks evidence on the influence of firm size and type on the power to change the SLA, as public organizations have the power to change the SLA under the regulatory requirements, whilst small organizations do not.

IT infrastructure: The literature reported that CC services are standardized (Schneider & Sunyaev 2014) and has emphasized that standardized processes are the ones that are ready and likely to move to the cloud (Lacity & Reynolds 2014; Loebbecke et al. 2012). The empirical findings corroborate what the literature has documented, and relate the challenge of standardized CC services to the maturity of the organization's processes (i.e., standardization of the processes). Perhaps organizations need to be oriented towards standardizing of their processes rather than just moving the already standardized processes to the cloud, because the unstandardized processes may be the ones that need to be moved to the cloud. The IT infrastructure can be *"a significant barrier or enabler in the practical options available to planning and changing business processes"* (Broadbent et al. 1999, p.158). This implies the need for collaborative efforts between the client organization and the CSP. This collaboration has to focus on identifying the organization's

readiness (Swanson 2010) and setting a modernization initiative for its IT infrastructure, which, in turn, will facilitate change management of its business processes and minimize disruptions or delays (NTT Europe 2013). This implies the need for developing frameworks for assessing cloud-readiness of organizations, not only large organizations with global presence (Loebbecke et al. 2012), but also SMEs that operate at the national level.

CC Adoption Strategies

According to the literature, existing studies have focused extensively on various factors that determine cloud sourcing decisions (Schneider & Sunyaev 2014); such a focus has been more on the technical than the institutional factors (Yang & Tate 2012; Schneider & Sunyaev 2014). The literature also focused on readiness assessment (Loebbecke et al. 2012), capabilities offered by CC (Iyer & Henderson 2012; Iyer & Henderson 2010), and practices to overcome CC adoption challenges, such as educating stakeholders, matching CC services to existing needs, finding the right CSP, and building client-provider relationships, and acquiring the adequate skills (Lacity & Reynolds 2014). However, there is less focus on how various CC adoption strategies are shaped by combinations of institutional factors that are related to a wider social system of various involved parties.

The literature has focused solely on CC adoption strategy that is driven by the desired efficiency and cost reduction (Venters & Whitley 2012; Schneider & Sunyaev 2014), and lacked focus on gaining legitimacy, that is beyond imitating legitimate peer organizations, as a drive for CC adoption (Pfaller et al. 2013; Hustad & Olsen 2012). Additionally, the literature advocated the need to *"provide evidence for the underlying mechanisms driving differences, for instance, between adopter and non-adopter firms"* (Schneider & Sunyaev 2014, p.16). In addition to the institutional factors identified, the thesis suggests three strategies that distinguish between different CC adopters. These strategies are driven by efficiency or legitimacy, and finally a non-adoption strategy that is driven by lack of trust and an unclear vision.

7.1.2. Neo-institutional theory

The literature review I presented in Paper2 suggested the need to understand the factors that affect the adoption of CC and how enterprises respond to external and internal pressures and why. Thus, an empirical study can benefit from using the institutional theoretical perspective that *"offers several unique insights into*

organization-environment relations and the ways in which organizations react to institutional processes." (Oliver 1991, p.151). Indeed, the intended institutional stance here is the "neo-institutional" stance that rejects the notion of the "rational actor"; it follows that organizations' choice or nonchoice are influenced by *"state, societal, and cultural"* forces (Oliver 1991, p.151) to legitimate themselves within their environment, rather than to serve their own interests in efficiency (Oliver 1991; DiMaggio & Powell 1983; Powell & DiMaggio 1991). Hence, this thesis is aimed at understanding the CC adoption phenomenon in its social setting using neo-institutional theory. In so doing, this thesis responds to calls to use neo-institutional theory to study the adoption of IS/IT innovations from the perspective of a broad social system, rather than a single organization (e.g., sector, or country) (Currie 2009).

I do not claim that I have added significantly to neo-institutional theory; nor have I made major changes. Rather, I used the theory to explain how CC adoption is influenced and reflected through the adoption strategies chosen in order to better understand the CC adoption phenomenon. According to Harlow (2010), applying a theory to a new context is counted as a contribution to that theory. Furthermore, the empirical findings that offer insights for theoretical implications, which deserve further validation in the future, count as contributions (Ågerfalk 2014). I applied the theory to new contexts, such as countries (i.e., Egypt and Norway) than it was originally applied to understand a single organization (Currie 2009); hence, this can be counted as a contribution to theory, as new empirical findings from the two case studies emerged to suggest further theoretical implications beyond the existing research context.

This broad focus on countries gave an insight into what constitutes the institutional factors that influence the adoption and non-adoption of CC services. This thesis also responds to the need to explore the "reasons" behind conformity and non-conformity to the institutional norms and rules when organizations choose to pursue a certain strategic response (Oliver 1991).

Neo-institutional theory offers a useful lens, because it is related to the cultural influences on decision-making that are based on the notion that: *"organizations and individuals who populate them are suspended in a web of values, norms, rules, beliefs, and taken-for-granted assumptions, that are at least partially of their making"* (Barley & Tolbert 1997, p.93). In the context of this thesis, these values, norms, rules, and beliefs are shaped with regard to CC adoption. Hence, in this thesis, I argue that CC

adoption is an institution that is socially constructed and maintained through interactions between actors (or organizations) at the field level (Barley & Tolbert 1997). The constraints or opportunities brought by those actors determine the organizations' behavior (i.e., decisions) towards CC adoption. This is what we, as IS researchers, need to learn from organization studies' theory, such as neo-institutional theory (Orlikowski & Barley 2001). We need to shift focus from the *"the technical and practical exigencies of implementing and operating information systems"* to investigate how the regulative, normative, and cultural systems shape the adoption of IS, and give *"cognitive and cultural explanations for organizational responses"* (Orlikowski & Barley 2001, pp.152–153).

What we do know about the neo-institutional theory from IS literature is that the organizational field and legitimation strategies were not utilized, yet, for studying IS/IT adoption phenomena (Mignerat & Rivard 2009). In this regard, our existing knowledge is limited and more studies are needed *"to investigate situations where the targets of institutional pressures enact responses other than the acquiescence strategy"* (Mignerat & Rivard 2009, p.389). Furthermore, IS literature advocated the need for examining the institutional influences in the context of outsourcing-type arrangements (Weerakkody et al. 2009).

Our knowledge about CC adoption in light of the institutional perspective is, yet, limited (Schneider & Sunyaev 2014). Positivist studies proved that the competitors (Messerschmidt & Hinz 2013), and the successful adoption by peer organizations (Xin & Levina 2008) serve as mimetic influences on the adoption of CC. A qualitative study focused on the vendor side claimed that, as the CC market legitimates by time, vendors develop political strategies to shape the evolution of the CC market (Su 2011). Furthermore, a positivist study focused on how the institutional influences affect the client organization's perception of CC characteristics (e.g., accessibility, scalability, cost-effectiveness, and lack of security) (Saya et al. 2010). On one hand, the positivist stance dominated CC research using neo-institutional theory. On the other hand, institutionalists advocated the *"need to move, however slightly, away from strictly positivist research and incorporate interpretivist methods that pay serious attention to the subjective ways in which actors experience institutions"* (Suddaby 2010, p.16).

This thesis complements the existing research stream by bringing in the concepts from the neo-institutional theory to analyze the findings from two interpretive case studies to explain the adoption of CC. To identify the constituents of the institutional factors

that represent CC adoption constraints and opportunities, I used the organizational field concept (Scott 2001) as a template to define the external organizations that have influence on CC adoption. These organizations were identified from Egypt and Norway case studies and the Delphi study's follow-up interviews, and included governments, CSPs, traditional IT providers, and media. The influence of these organizations is explained through the concept of isomorphic pressures (i.e., coercive, normative, and mimetic) (DiMaggio & Powell 1983), which caused organizations to pursue various CC adoption strategies. These CC adoption strategies included efficiency-motivated adoption, legitimacy-motivated adoption, and non-adoption of CC services. I offered an explanation for these strategies using the five strategic responses put forward by Oliver (1991) (i.e., acquiescence, compromise, avoidance, defiance, and manipulation). These strategic responses have been noted interchangeably as "strategies" and "strategic behaviors" in the literature (Mignerat & Rivard 2009; Oliver 1991). This approach to strategy is called "systemic", which looks at the strategy as a social action that needs to be understood within its social context (Bakir & Todorovic 2010). The systemic approach emphasizes that the strategy is *"inescapably linked to the cultures and powers of the local social systems in which it takes place"* (Whittington 2001, p.2).

The institutional perspective holds that an organization's response to the isomorphic pressures is bound by organizational conflict, resources, and awareness (Oliver 1991). As suggested by Oliver (1991), it also holds that an organization's response to isomorphic pressures depends on these pressures per se. Below, I attempt to explain the links between: (1) the pressures exerted from the external environment (i.e., the organizational field), (2) strategic responses and the dominant reasons behind them, and (3) the identified institutional factors and CC adoption strategies. Figure 16 demonstrates these links.

Common patterns emerged among the isomorphic pressures and other field-level changes exerted from the external environment (i.e., the organizational field); thus, I grouped them into the category of "external institutional factors", so that I could explain the various influences of these factors. Likewise, the pressures exerted from within the organization are grouped into the category of "internal institutional factors". They could not be explained by the isomorphic pressures that have commonly been exerted by the external environment (DiMaggio & Powell 1983).

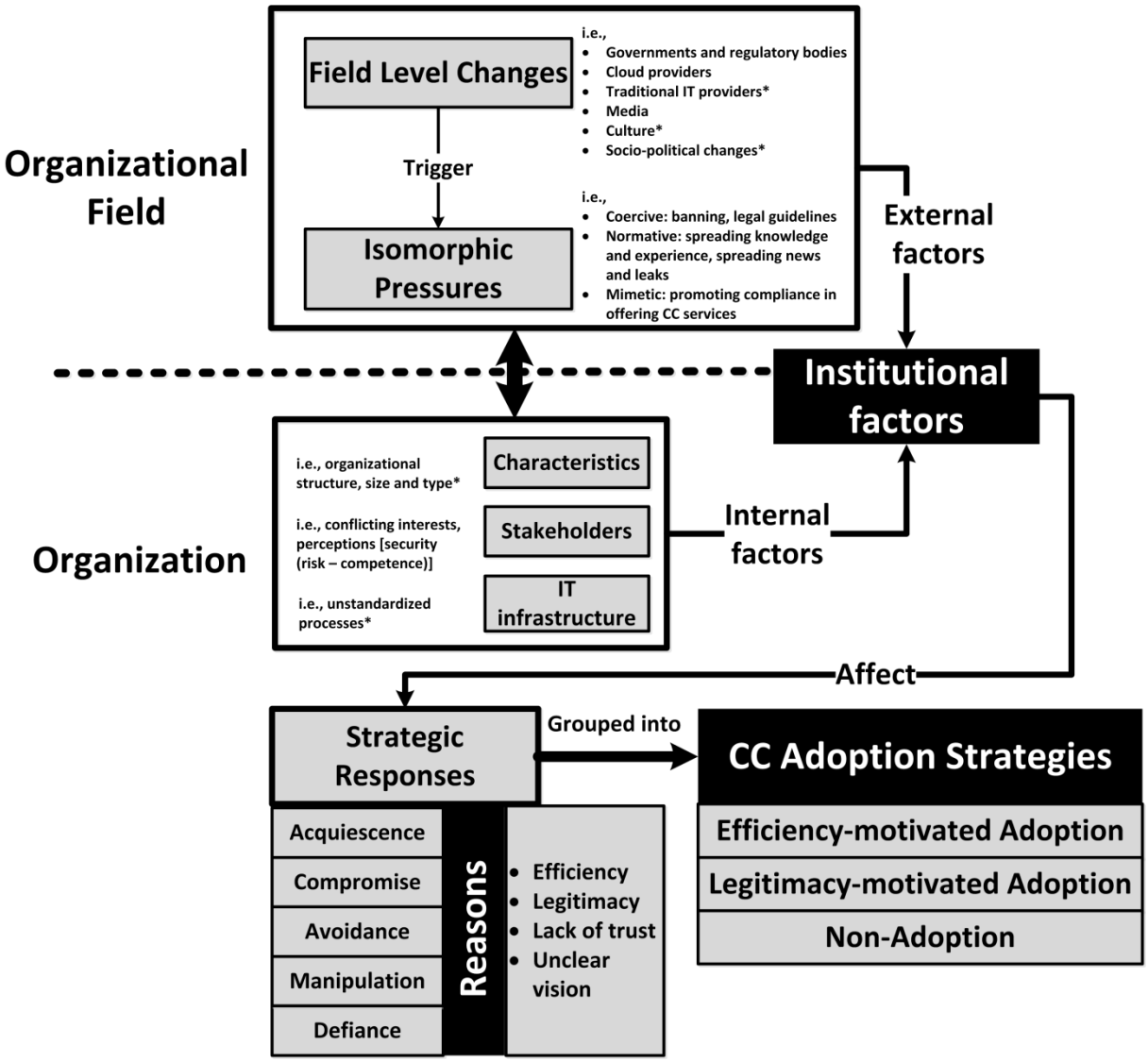


Figure 16: Contributions in light of the neo-institutional theory
Bullets ending with (*) are explained in the subsequent paragraphs

In the literature on neo-institutional theory, government regulations have been always reported to have a coercive influence, which constrains organizations in adopting certain practices or organizational models (DiMaggio & Powell 1983). This corroborates the findings from the case study of Norway. However, the findings from the case study of Egypt indicated that the government had a rather normative influence on organizations towards adopting CC by spreading knowledge and experience through public sessions and panels. This finding provides implications regarding the claim that institutional influences *"tend to derive from different condition and may lead to different outcomes"* (DiMaggio & Powell 1983, p.150). The literature on neo-institutional theory and IS/IT outsourcing reported that the media had a mimetic influence that accelerated the diffusion of IS/IT outsourcing practices (Hu et al. 1997).

However, the findings indicate a rather normative influence of media that decelerated the diffusion of CC services by distributing information about the Snowden leaks.

The literature on IS/IT and neo-institutional theory suggested that the future research needs to focus on the political view of the institutional influences *"that includes key components such as power, politics and various actors"* (Mignerat & Rivard 2009, p.389). Regarding the external factors, the traditional IT providers together with CSPs had a combined effect that manifested itself in the political game. As explained in sub-ection 6.1.1, this political game had a confusing influence on the clients, and no immediate effect traced with regard to a particular strategic response; however, as one of the informants pointed out, it is an important matter to take into consideration. The limited literature on CC and neo-institutional theory had focused on the provider side and the strategies that traditional IT providers take to adapt to the emergent and evolving market of CC, by transforming themselves into CSPs (Su 2011). However, the findings indicate that traditional IT providers follow a reverse strategy by running negative marketing strategy against CSPs about CC security problems to discourage their clients from moving to CC solutions.

The literature on neo-institutional theory (DiMaggio & Powell 1983), and on CC and neo-institutional theory (Xin & Levina 2008) claimed that peer organizations have the tendency to be copied by organizations in situations of uncertainty. However, the findings indicated a further mimetic influence of local CSPs, who take opportunity to demonstrate their regulatory compliance over global CSPs, on organizations to move to their CC services and dismiss global CSPs.

At the organizational field level, the socio-political changes are better explained as a factor; this factor did not have a direct influence related to CC in particular. Rather, it was related to the political reform movements found in the Egyptian context. It contributed to an increase in the lack of trust, which led to cases of non-adoption of CC services in the case study of Egypt. The literature on neo-institutional theory (DiMaggio & Powell 1983), and on CC and neo-institutional theory (Saya et al. 2010) claimed that the institutional influences are exerted by organizational actors who have a common meaning system and frequent interactions with the influenced organization. Precisely, those actors have a direct stake with the influenced organization, such as customers, suppliers, partners, government, industry and professional organizations, and competitors. However, the findings indicate that even changes in a broad and complex social system can inhibit the organization from adopting CC services, such as

revolutions and their consequences, where actors (e.g., political parties, protesters, etc.) may not have a direct stake or a frequent interaction with the influenced organizations.

Culture of the society around the common sense of not accepting the data to be off-premise despite data security is technically guaranteed. This factor can have an inhibiting influence leading to non-adoption. The findings regarding this factor corroborate the literature on the neo-institutional theory claiming that institutional influences can be exerted *"by cultural expectations in the society within which organizations function"* (DiMaggio & Powell 1983, p.150). However, the literature on CC and neo-institutional theory lacked the focus on cultural matters (Saya et al. 2010; Xin & Levina 2008), which can have an important influence on CC adoption.

In the literature on neo-institutional theory, organizations are more likely to dismiss the institutional influences exerted by the external environment when *"internal objectives diverge or conflict very dramatically with institutional values or requirements"* (Oliver 1991, p.156). Furthermore, the conflicting expectations of internal stakeholders lead to misaligned and conflicting strategies (Lacity & Hirschheim 1995). This corroborates the findings that indicate conflicting interests of internal stakeholders that served as an inhibiting factor leading to unclear vision and, thus, resulting in non-adoption. IS managers used to follow accommodation strategies that compromise on cost and service (i.e., persuasion that IS can improve performance at a minimal cost) (Lacity & Hirschheim 1995). However, the findings indicate that this is not always the case, which implies that accommodation strategies need to be focused on the notion of *"following fashion can legitimize organizations and their leaders regardless of performance improvement"* (Wang 2010, p.63).

The internal institutional factors, namely, organization characteristics and IT infrastructure have been better discussed against the literature backdrop in sub-section 7.1.1. Furthermore, no immediate effect of some institutional factors (e.g., organization characteristics and IT infrastructure) was found with regard to a particular CC adoption strategy. However, some other institutional factors (e.g., government regulations, government banning, and socio-political changes) had an immediate effect on a particular CC adoption strategy. The reasons found to be driving CC adoption strategies are: maintaining efficiency, maintaining legitimacy, lack of trust, and unclear vision.

From the institutional perspective, rationality is linked to the search for efficiency, while irrationality is linked to the search for legitimacy (Mignerat & Rivard 2009). Efficiency encompasses technical and economic efficiency, where organizations can achieve better outputs with lower costs, less effort, and better hardware and software (DiMaggio & Powell 1983; Kshetri 2013). Legitimacy is *"socially constructed in that it reflects a congruence between the behaviors of the legitimated entity and the shared (or assumedly shared) beliefs of some social group"* (Suchman 1995, p.574). Irrationality in the neo-institutional perspective implies seeking legitimacy through the congruence with either legal mandates, or cultural norms and meanings (Deephouse & Suchman 2008). Hence, I categorized CC adoption strategies into efficiency-motivated adoption, legitimacy-motivated adoption, and non-adoption. An unclear vision and a lack of trust resulted from the external (such as socio-political changes and culture) and internal factors (such as conflicts among stakeholders). These institutional factors led to non-adoption, despite the fact that organizations intended to adopt CC services and had the opportunity to do so.

The abovementioned three strategies were derived from the strategic responses, or strategies, proposed by Oliver (1991) to fill in the void that have always been a point of criticism for the institutional theorists, who *"have tended to overlook the role of active agency and resistance in organization-environment relations"* (Oliver 1991, p.151). Thus, there is a need for examining the available strategies for organizations to respond to the institutional environment. In the following, I discuss the three derived CC adoption strategies in light of the neo-institutional theory and the five strategies proposed by Oliver (1991). It is suggested that these strategies vary in the degree of responsiveness depending on the institutional influences exerted on the organization (Oliver 1991).

Starting with the acquiescence strategy, imitation is one tactic of this strategy that may involve unconscious mimicry of institutional models, which is the CC model in the context of this study. This was the case of Narvik municipality, when they first started using Google Apps without questioning about the location of the data. Narvik aimed at using CC services to replace their old outdated IT environment and achieve efficiency. The acquiescence of an organization depends on the degree of its consciousness in following the institutional influences, its awareness of the institutional influences, and its expectations that following the institutional influences will serve its own interests (Oliver 1991). Narvik municipality was aware of the CC services offered by the CSPs that are expected to serve its own interest of seeking efficiency. However, Narvik

municipality was not aware of the institutional influence of the regulatory body (i.e., Datatilsynet in this case) and did not have information about where Google is storing the data, thus, the municipality failed to maintain its legitimacy within its legal legitimation system. This led Datatilsynet to ban the use of Google Apps until the municipality conducts risk assessments and gets information about the location of the data. The story of Narvik implies that efficiency was attained, but legitimacy was not, thus, it has been interpreted as an efficiency-motivated strategy.

This finding has three theoretical implications that deserve further validation in the future. First, legitimacy is subjective at times and it manifests in subjects, or levels, of legitimation; a subject of legitimation can be a system of power (i.e., power of coercion) (Deephouse & Suchman 2008). Perhaps using Google Apps unconsciously has legitimated the municipality within the CC market, which is a low-level subject of legitimation, but has not legitimated it within the high-level legitimation subject that is the Norwegian legal system. These multiple levels of legitimation subjects demonstrate the complexity of the real world and have been argued to be a challenge for researchers to investigate (Deephouse & Suchman 2008). Second, the finding corroborates the claim that the acquiescence is likely to happen when the expected efficiency is attainable, however, it proves the opposite to the claim that acquiescence is likely to happen *"when the degree of legitimacy attainable from conformity is high"* (Oliver 1991, p.159). Third, it has been claimed that the proposed strategies by Oliver (1991) explain variations of organizational responses to the institutional influences. However, it would be insightful to develop further institutional concepts, in the future, to explain the implication of a strategic response to create an institutional influence (i.e., the banning that resulted from the Narvik's acquiescence).

In the case of client C1's organization, they expected to attain agility, which, in turn, means the organizations' ability to adapt to market changes in a productive and cost-effective manner. Hence, this agility-driven adoption was interpreted as efficiency-motivated strategy. However, C1's organization did not consider a well thought assessment of its cloud-readiness, which delayed them and did cost them time and effort to implement adapters at their IT legacy environment. This corroborates the call for using neo-institutional theory to study *"the synergy between internal IS/IT capabilities and external skills that consultants bring to organizations"* and *"the outcomes of the relationship between the two parties"* (Weerakkody et al. 2009, p.366).

Interestingly, compromise, avoidance, and manipulation strategies have induced a legitimacy-motivated adoption; according to Oliver (1991), these strategies are likely to happen when the anticipated legitimacy or efficiency gain from conforming to the institutional influence is low. The compromise strategy indicates that the organizations are often confronted with conflicting institutional constituents for which organizations attempt to have an open negotiation with the external environment (Oliver 1991). The compromise strategy enacted by client C4's organization was an attempt to negotiate sourcing strategies and choose the right sourcing partners to accommodate the legal conflict that requires dealing with CSPs who provide data storage within the EU region. C4's organization was not allowed to deal with CSPs from India; hence, its legitimacy gain would have been low. Thus, the compromise strategy enacted by C4's organization was legitimacy-motivated to accommodate its selection of CSPs with the legal requirements.

In another two initiatives toward CC adoption, C4's organization was conducting a proof-of-concept (POC) of CC solutions. The reason for POC initiatives is that the organization had so many interdependencies between its legacy systems and moving to the cloud immediately may cause performance degradation of its operations and affect its service quality negatively. Thus, its anticipated legitimacy, as an organization operates in healthcare sector, would have been low among the patients. This finding corroborates the logic of avoidance strategy that is *"the organizational attempt to preclude the necessity of conformity"* by concealing *"nonconformity behind the facade of acquiescence"* (Oliver 1991, p.154). Furthermore, according to the institutional perspective, an organization tends to resist the institutional influences exerted *"to improve its efficiency if it has doubts about the impact of [these institutional influences] on the quality of its services"* (Oliver 1991, p.161), which, in turn, has some ramifications on its anticipated legitimacy in case of conformity. Thus, the CC adoption strategy enacted by C4's organization was legitimacy-motivated.

Manipulation strategy follows that organizations may tend to *"shape and redefine institutionalized norms"* of acceptable practices or performance (Oliver 1991, p.159). Although the literature reported the growth in the market of public cloud services (Venters & Whitley 2012), because of the cost reduction and scalability benefits (Schneider & Sunyaev 2014). Not all organizations view public cloud services as an acceptable model for their business. This corroborates the claim that *"a one-size-fits-all approach may not work for all user organizations' cloud adoption. [Thus], organizations may have to make decisions"* regarding various cloud service models

(i.e., public, private, or hybrid) that fit their business (Kshetri 2013, p.383). The literature on CC adoption reported that private clouds are better when it comes to security and compliance with regulatory requirements (Schneider & Sunyaev 2014). For the organization where clients C2 and C3 work, implementing own private cloud model was an appropriate option for a number of reasons; first, they have not found any reference case of a wide use of public PaaS model in Europe. Second, they preferred to be independent of external support that may delay them in case critical bugs in the cloud system arise, which can demolish their image within their institutional environment. Thus, and thirdly, they aimed at preserving their image by implementing a private cloud model. This, again, represents a more active resistance to the institutional influences to improve its performance or economic fitness at the expense of threatening its legitimacy (Oliver 1991). Thus, for (C2 and C3)'s organization, adopting public cloud services is perceived to make its legitimacy gain low, which corroborates Oliver's (1991) suggestion that manipulation happens when the anticipated gain of efficiency or legitimacy is low. Hence, the CC adoption strategy of (C2 and C3)'s organization (i.e., implementing private cloud model) was legitimacy motivated.

The non-adoption strategy of CC services was induced from the defiance strategy proposed by Oliver (1991). The defiance strategy follows that organizations may tend to dismiss or ignore the institutional influences in either one of the two situations; the potential for external institutional influences *"is perceived to be low or when internal objectives diverge or conflict very dramatically with"* the institutional influences (Oliver 1991, p.156). The two situations were evident from the two case studies; the case study of Egypt provides an example of the first situation, where the potential of adopting CC services is perceived to be low as a result of the lack of trust. This lack of trust resulted from the high environmental uncertainty (i.e., socio-political changes and lack of legal framework), which proves the opposite to Oliver's (1991) suggestion that defiance is likely to happen when the environmental uncertainty is low. However, culture is proved to be a reason for defiance, which implies low environmental uncertainty as suggested by Oliver (1991).

The case study of Norway provides an example of the second situation, where the internal objectives diverge among the internal stakeholders and conflict with the CSP's influence towards adopting CC services. These divergent and conflicting objectives resulted from the bureaucratic structure and the divergent knowledge and interests of the stakeholders, which induced unclear vision towards adopting CC services. This

finding corroborates the two suggestions put forward by Oliver (1991) that the defiance is likely to happen when the multiplicity of constituent demands is high and the environmental uncertainty is low. Hence, the findings from the two case studies were interpreted as a non-adoption strategy.

To conclude, the findings have been discussed in light of the neo-institutional theory in this sub-section. The findings are not claimed to offer significant contribution to the theory, rather, they provide empirical insights that offer theoretical implications. Indeed, the findings are not yet generalizable to other contexts, thus, the theoretical implications deserve further systematic validation.

7.2. Implications for Practice

The thesis contributes to practice; the Delphi study identified 55 issues of concerns regarding adoption of CC. These issues were further grouped into 10 categories in terms of (1) security, (2) availability, (3) migration, (4) business, (5) legal and ethical concerns, (6) culture, (7) awareness, (8) impact, (9) strategy, and (10) IT governance. These issues are important for decision-makers to take into account when considering CC investments.

CC services are here to stay and all stakeholders (i.e., clients, providers, and regulators) need to be prepared to foster the adoption of these services. The identified institutional factors and adoption strategies may serve as lessons for client organizations to consider the ongoing dynamics in the external environment (i.e., legal, cultural, and political) to make more informed decisions. Hence, organizations can avert unwanted consequences that may cause a bad adoption experience of CC services.

To conclude this thesis, I will describe the implications for clients, providers, and regulators; these implications are summarized in Table 19.

Table 19: Summary of implications for practice

Implications	Description
For clients	-Need to consider the ongoing dynamics in the external environment to make more informed decisions and avert unlikely consequences. -Need to have a business case that is driven by business needs rather than IT costs. -Need to conduct a good estimation of the required change and communicate it with internal stakeholders in a convincing way to avoid having unclear vision and delays in executing the adoption strategy.

For cloud providers	- Need to be strategic in sensing different demands in different markets, and reflecting these demands in their marketing campaigns to regain the market's trust. -Need to consider clients' security requirements, which differ from the security they offer.
For law-makers	-Need to learn from the financial industry about how to build an eco-system for exchanging data, instead of money, globally in the cloud based on trust and international governance practices.

A recent report showed that organizations are confused about which applications should go to the cloud, which implies some signs of unclear vision (NTT Communications 2015). Furthermore, the findings from this thesis showed that the internal stakeholders have a major role in reaching a clear vision and managing the change. For clients, there is a need for a business case that is driven by business needs rather than IT costs and based on a good estimation of the required change in an organization. This need for change has to be communicated to the internal stakeholders, including owners, managers, and employees; this is to avert conflicts in interests and guarantee a clear vision regarding which processes should be moved to the cloud.

Change is perceived by clients as a threat rather than an opportunity; thus, clients tend to resist opportunities to use CC services rather than look at them. This issue was ranked as number six by providers and should not be underestimated. Change extends to the competence, business model, organizational structure, processes and routines (as discussed in Chapter 6).

Once the required changes have been estimated, plans need to be in place regarding change management and migration management. This is important if an organization is to have a good migration experience without delays.

The external environment surrounding the adoption of CC is full of turbulence, which create inhibiting and constraining factors that can exceed the enabling ones in some contexts. Thus, uncertainty is increased and clients are left confused. This is a result of an immature CC market, which is also affirmed by recent statistics that the majority of decision-makers are not really sure about the potential of CC services (NTT Communications 2015). Furthermore, what happens in the media nowadays increases the lack of trust from the clients' side. Together with differences in regulatory requirements, this poses a challenge for CSPs and requires them to be strategic in

identifying different demands in different markets, and reflecting these demands in their marketing campaigns. Furthermore, the findings of this study imply that CSPs need to consider how clients' security requirements differ from the security they offer. These security requirements may go beyond the technical dimension (e.g., encryption); they may be physical (e.g., location of the data), ethical (e.g., standards for a particular industry), or social (e.g., lack of trust in and fear of unknown CSPs at the local scale), as asserted by the majority of clients and providers in my study.

However, this does not imply that security is only the CSPs' responsibility; CloudLock's statistics show that 1% of the client organizations' employees are responsible for 75% of cloud security risks within the organization through data sharing with outside collaborators (Donnelly 2015).

The development of regulations is not moving as fast as technological developments in the CC industry. This manifested itself in the slow development of regulations in Norway case study and upgrading the legislative system based previous cases in the Norwegian context. This also includes the situation in Egypt case where there are no regulations in place yet, despite the structure of the legal authority is already sketched. The local regulations are undoubtedly important to be in place; however, international governance practices for CC industry are equally important. The lack of IT governance practices was ranked as number eight concern by providers. For regulations to be mature with relation to CC, lessons can be learnt from the financial industry and how they built their eco-system for exchanging money globally based on trust and international governance practices. Although the financial industry has achieved a sustainable cloud eco-system, this happened at the national level rather than at the global level (Eaton et al. 2014). Law-makers in the area of CC have been called to consider mimicking the financial industry with regard to governance in order to address the lack of trust by clients.

“We can only see a short distance ahead, but we can see plenty there that needs to be done.”

— Alan Turing

8 Conclusion, Limitations, and Future Work

This chapter summarizes the findings of this thesis, highlights the limitations related to the generalizability of the findings and use of theory, and offers avenues for future research.

8.1.Summary

This thesis explores the institutional factors that influence the shaping of CC adoption strategies and our understanding of the phenomenon of CC adoption. The main RQ raised in Chapter 1 focused on our gaining a better understanding of the phenomenon of CC adoption: "How can we understand the phenomenon of CC adoption within organizations?" To address this research, I reviewed the literature on CC adoption and neo-institutional theory to understand existing research contributions in the area under study and to define the scope of my study. This was articulated in Paper1 and Paper2. In addition, I referred to the IS/IT outsourcing literature, as shown in Chapter 2 (See Sections 2.1 and 2.2), because CC is an emerging IS/IT outsourcing model.

Then, with my understanding of the existing research stream and the use of neo-institutional theory in the context of CC (See Section 3.3 in Chapter 3, Paper1, and Paper2), the main RQ was addressed by conducting a Delphi study and two case studies. These were used to explore the institutional factors (both external and internal) that can be seen to have an important influence on CC adoption and the shaping of adoption strategies. This work has been articulated in Paper3, Paper4, and Paper5 to address the two SQs: "What are the institutional factors that affect CC adoption in organizations?" and "How do institutional factors shape CC adoption strategies?" The institutional factors and their important influence were identified through interviews and rankings. These factors are related to various contexts such as the country, the CC business environment, and the client organization. Five external factors were identified, which are related to the external social environment, both local and global (i.e., governments and regulatory bodies, cloud providers (or CSPs), media, socio-political changes, and culture). Three internal factors were identified; these are related to the internal social and technical environment of an organization (i.e., internal stakeholders, firm characteristics, and IT infrastructure). Furthermore, this thesis identifies three CC adoption strategies: efficiency-motivated adoption, legitimacy-motivated adoption, and non-adoption.

The identified institutional factors have various influences (e.g., enabling, constraining, inhibiting, guiding, and confusing) that, eventually, shape CC adoption strategies. The institutional factors and CC adoption strategies are discussed in Chapter 6 with regard to the existing literature. An explanation of the influence of each factor or combination of several factors has also been given.

It should be noted that some institutional factors were identified, but no immediate effect could be traced with respect to a particular strategy. However, according to one of the informants, it is important to take those factors into consideration. For example, in the CSPs factor, it was found that the political game going on between the CSPs and the traditional IT providers can influence the adoption of CC services.

8.2. Limitations and Generalization Issues

The limitations of my research approach and its validity issues in terms of data collection and analysis have been discussed in Chapter 3. In this section, I discuss limitations regarding the generalizability of the findings from my research. My research approach is interpretive, and generalizability in interpretivism differs from that in positivism (Lee & Baskerville 2003). In interpretivism, *"the goal of universal laws is inappropriate in the study of human affairs because individuals, groups, and other social units are all unique, and therefore demand idiographic theorizing instead"* (Lee & Baskerville 2003, p.229). Thus, generalizations from interpretive research *"should […] be seen as explanations of particular phenomena […] in specific IS settings, which may be valuable in the future in other organizations and contexts."* (Walsham 1995, p.79). Lee and Baskerville (2003) highlighted four types of generalization from interpretive research as suggested by Walsham (1995), which involve generalizing empirical facts and descriptions to concepts, a theory, implications, or rich insight.

I position my findings as generalizable in terms of developed concepts, such as institutional factors (external and internal) and CC adoption strategies (efficiency-motivated, legitimacy-motivated, and non-adoption). Furthermore, the discussion of the findings was done in light of the neo-institutional theory and the previous literature. This offered interesting and rich insight into CC adoption phenomenon and theoretical implications that deserve further validation in the future. These implications offer tendencies rather than predictions. In the following, I discuss some issues related to generalizability and use of theory:

- The findings from the Egypt and Norway cases provided explanations of various institutional factors that are related to each context and how they shaped CC adoption strategies in each context. The possibility to generalize these institutional factors to other contexts is still a limitation. These factors and their influence can differ from one context to another; thus, further examination is needed.

- The Delphi study is post-positivist (Day & Bobeva 2005) and is combined with follow-up interviews in my research approach. This gave rich descriptions of the findings. Findings from the Delphi study can be generalized (i.e., are valid for other contexts) to some extent as the lists of 18 CC adoption issues were identified and ranked by three subpanels, which comprised informants from different domain backgrounds, countries, and types of organization. Although the Norwegian informants dominated the sample, some of them worked for organizations that had a global scope. Again, the generalization of the findings from the Delphi study may be more relevant to the Norwegian context.

- Experiences and questionnaire responses solicited from informants between September 2013 and March 2015, helped to improve our understanding of the CC adoption phenomenon and the dynamics of its context. However, these experiences may differ for the period following the data collection. Experiences can also differ as client organizations progress in their adoption of CC services, or as informants' roles changed from a client perspective to a provider perspective and vice versa.

- Neo-institutional theory was used in my research to analyze the collected data. This involved coding the data using concepts such as isomorphic pressures (DiMaggio & Powell 1983) and strategic responses (Oliver 1991). These concepts helped me to understand and explain the various institutional factors and adoption strategies, particularly when analyzing the data collected from new contexts in the two case studies. Within the external environment that surrounds an adopting organization, some factors have influences that are neither coercive nor normative or mimetic. These factors could not be coded using concepts from neo-institutional theory; for instance, the confusing influence of the political game played between traditional IT providers and pure-play CSPs.

8.3. Future Research

The contribution of this thesis and its limitations offer opportunities for future research. The external institutional factors and their influence are worth investigating in a comparative manner (e.g., across different countries and different sectors). A comparative analysis could be used along with new theoretical lenses such as "management fashion" which offers an opportunity as an analytical lens in the future research (Abrahamson 1996). This lens can provide an insight into how fashion-setters (i.e., CSPs, consultants, governments, and academics) sense different market demands and how they respond to these demands in their promotion of CC services. Such insights can have implications for research and practice.

The focus of this thesis was at a broad institutional level in identifying external and internal institutional factors and their influence on CC adoption strategies. Future research should focus on more technical levels by identifying factors that influence the adoption of particular service models (e.g., SaaS, PaaS, and IaaS or public, private, and hybrid). Such contributions can illuminate the decision-making process.

To identify more internal institutional factors, future research should focus on the development of business cases and good practices for change management. Such contributions can provide an understanding of the evaluation and integration or implementation processes. Longitudinal studies on CC adoption are lacking in the literature (cf. Paper2); nonetheless, they can highlight valuable implications for the entire CC adoption experience.

Finally, the results from the Delphi study offer a wide range of topics for future research. The identified categories and related issues of security, strategy, impact, legal and ethical, business, IT governance, culture, awareness, migration, and availability, provide possibilities for both qualitative and quantitative research studies.

“Imagination should be used, not to escape reality but to create it.”
― Colin Wilson

9 Reflections

"From CC security to CC adoption factors and strategies, and a rather different outlook on security!"

At the outset of my research journey, my focus was on security in the cloud and the development of a model for securing enterprise data in the cloud. The aim was to pursue security in the cloud from a technical point of view (e.g., through encryption and standards). As my knowledge matured throughout the PhD program, my focus drifted to a broader view on CC, which is the CC adoption phenomenon. My focus has widened as a result of my research activities, which ranged from taking courses on research methods for identifying research gaps and exploring the field, to attending workshops for discussing my ideas with peers, and undertaking a systematic literature review. This led me to question: "Is it all about technical security in the cloud?", and "What are other areas within the CC topic that need further exploration?" I had these questions in mind while I was reviewing the literature. While I was at early stage of surveying the literature on CC, I came across a review article by Yang and Tate (2012); the authors indicated that the technological issues that were covered mostly include security, and argued that these technological issues are difficult to read and do not offer practical knowledge for business professionals. The review raised a call for more IS studies on CC adoption that offer implications for business users in business-friendly language.

This motivated me to focus the scope of my research on CC adoption. My systematic review of IS studies on CC adoption indicated gaps in case studies that utilized institutional theory and Delphi studies to explore such a phenomenon. My empirical work began with the Delphi study. My aim was to explore the CC adoption phenomenon by identifying and ranking the most important issues (or topics) related to CC adoption in enterprises. I used the terms "enterprises" and "organizations" interchangeably in my research. The process of the Delphi study took one year and eight months, including the Delphi surveys and follow-up interviews. During the Delphi brainstorming survey and follow-up interviews, the inputs from the informants were rich, particularly bearing in mind that the informants had different experiences related to their domain backgrounds. However, after the first ranking survey, the agreement level was very low and it was a challenge to move onto a second ranking round with the same list of 33 items. The rankings were not consistent among the subpanels; thus, it was difficult to have the same narrowed-down list for all the subpanels. At this point, there was no choice but to generate a different narrowed-down list of the top 18 items for each subpanel. This procedure differed from that used in previous Delphi studies of this kind where the ranked list was the same throughout the ranking rounds (Iden et al. 2011; Schmidt et al. 2001). However, the conditions of this study dictated a different approach.

The ranking results of the second ranking round did not indicate a strong agreement (rather, it was to some extent a moderate agreement). Ranking is stopped either when a significant and strong agreement is reached or when it is not reached (Iden et al. 2011). There was no opportunity to carry out more rounds of ranking after the majority of informants kept their old rankings, which were based on their individual experience of the phenomenon. This explains why a strong agreement was not reached: the Delphi study provided accounts for *"the inevitable variability of perspectives of people looking at the same phenomenon from different values and viewpoints at different points in time."* (Schacter & Coyle 1997, p.348). These different viewpoints brought to the table a rich body of opinion on the available alternatives that inform decision-making. However, they did not help to generate a significant consensus, nor were they useful in dictating decision-making (Franklin & Hart 2007; Turoff 1998).

Furthermore, the Delphi study provided rich insights into choosing the cases and the triangulation of the data, as explained in Chapters 4 and 6. I conducted the case studies in parallel with the Delphi study; thus, my research approach was neither linear nor sequential. I decided to use two case studies because some informants from the Delphi study provided interesting inputs relating to the Egyptian and Norwegian contexts. The unit of analysis of the case study is a phenomenon that is studied in relation to the dynamics of its social setting (Darke et al. 1998); in my research this is "CC adoption in the context of Egypt and Norway". Hence, the data from the two cases helped to identify context-related factors. I do not claim that I built a theory from these two cases, because theory cannot be built from fewer than four to 10 cases (Eisenhardt 1989). However, my cases did provide *"the basis for developing explanations of why a phenomenon occurs, and these may then be further investigated by applying them to additional cases in other settings"* (Darke et al. 1998, p.281).

There may be methodological issues in my research approach in the sense that there are signs of overlap between the two methods. In my research approach, triangulation occurred between the Delphi method and the case studies. The data from each method validated the data from the other; in other words, the ranking results were combined with data from the case studies to provide further explanations. Some factors were expressed by informants from both the Delphi study and case studies. In addition, each method allowed for new dimensions of the same phenomenon to be explored; for instance, some factors that emerged from the Delphi study would not have been found from the case studies, and vice versa. Thus, in addition to data validation, triangulation is useful *"not only to examine the same phenomenon from multiple perspectives but also to enrich our understanding by allowing for new or deeper dimensions to emerge"* (Jick 1979, pp.603–604).

The decision to use institutional theory in my research emerged from reading assigned articles on "theoretical foundations of information systems" course. Following this, I

reviewed the literature on the use of institutional theory in studying the adoption of IS/IT and IS/IT outsourcing (Weerakkody et al. 2009; Mignerat & Rivard 2009; Currie 2009; Ang & Cummings 1997), which advocated the use of institutional theory in studying the adoption of IS/IT and IS/IT outsourcing phenomena in a broader social system than a single organization. Furthermore, the literature called for exploring strategic responses to isomorphic pressures. Institutional theory is a theory of explaining and predicting (Gregor 2006). In the area of CC, I found the use of institutional theory was a work-in-progress and took a positivist stance for prediction purposes (i.e., hypotheses testing). This motivated me to use the theory to explain the findings that emerged from the two interpretive case studies. The theory enabled me to understand and explain various institutional factors that caused organizations to choose various CC adoption strategies.

Isomorphic pressures in the literature are exerted through a legal power (i.e., coercive), a learning process (i.e., normative), and by mimicking certain models (i.e., mimetic) (DiMaggio & Powell 1983). During the analysis of the data from the case studies some factors could be explained through the three isomorphic pressures; for example, the pressure of local Norwegian CSPs exerted a mimetic pressure on organizations to adopt CC services offered by them because they are safer and more legally compliant than global CSPs. However, some other factors identified from the Delphi study, such as the political game and its "confusing" influence could not be explained using isomorphic pressures. Thus, I categorized this political game factor and other factors as institutional factors instead of isomorphic pressures. Furthermore, this political game factor was identified along with its influence; however, I had no evidence of its immediate influence on the choice of a certain CC adoption strategy. This limitation can be further examined and developed in the future.

The findings from exploring CC adoption factors and strategies have provided insights into broader aspects of security other than the technical dimension, something that I have been interested in from the very beginning of my PhD research. These broader aspects include the legal dimension in terms of regulations and governments' reactions, and the social dimension in terms of the role of external social systems such as the media and CSPs in increasing the perceptions of internal stakeholders about potential security risks. In addition, the economic dimension of security emerged in that CC solutions can be secured but at a cost that may not be affordable for small organizations. Furthermore, the findings offered a view on security in terms of competence versus risk, which was not explicit in the literature.

Hence, the broad focus on CC adoption phenomenon allowed me to see other dimensions of security in the cloud. As Kenneth Burke stated in his book of permanence and change: *"every way of seeing is also a way of not seeing"*. These

broad dimensions of security offer possible opportunities for further examinations in the future.

It was surprising for me that a client in my sample had a different conception of what "being in the cloud" means! I had the interview with this client via Microsoft Lync. He asserted that his organization has not yet moved to utilize CC services yet, despite the fact that Microsoft Lync is basically a CC service! Nonetheless, this client's view was that his organization did not yet store their data on the cloud. An academic informant noted that the adoption of CC services does not necessarily require an explicit strategy, such as cloud-based communication tools and social media websites. Thus, it was interesting to observe these different interpretations. It may be that CC services became infused in our everyday life to the degree that we do not realize that we are actually using them, or it may be the case that individuals and organizations have started to build their own definitions of CC.

One more thought I have been pondering about is the link between CC and IS/IT outsourcing. If the term "CC" is replaced with "IS/IT outsourcing", what would differ and what would remain the same? The majority of my informants stressed the notion that "everybody talks differently about the same thing, which is CC". Furthermore, some informants treat CC and IS/IT outsourcing as one thing. Additionally, the literature treats CC as an emergent, but different, model from IS/IT outsourcing (Schneider & Sunyaev 2014).

From the standpoint of my interpretations of literature and my empirical work, I view CC and IS/IT outsourcing as "two sides of the same coin". I will now explain how this view has developed in my mind. In my opinion, both CC and IS/IT outsourcing involve a third-party that provides IT services for organizations that do not possess the necessary internal competence.

As demonstrated in Chapter 2, IS/IT outsourcing is a predecessor concept that is built on that notion. CC emerged as a synonym for the IS/IT outsourcing form known as SaaS (or ASP) that came along with the advent of the Internet. The netsourcing form emerged to offer a greater variety of IT services over the Internet than just software applications. The CC word came to light based on the same notion of SaaS and netsourcing.

My belief in the notion that CC existed 30 years ago is in line with that of many informants from the provider side. At that time, SaaS and ASP existed, and people have just started to name it the "cloud". This started with e-mail services, and then moved onto social media such as Facebook and storage services such as Dropbox. This was additional confirmation that CC is a new synonym for IS/IT outsourcing. This even made it clear that CC is just a business term associated with catchy words such as

efficiency, cost-reduction, agility, mobility, scalability, and competitive advantage. The majority of informants from the provider side, when asked how they defined the cloud, they kept telling me these catchy words. My take on this is that CSPs do not have a single widely agreed elaborate definition of CC; rather, and they just link it to words such as these for business purposes, so that their offerings are attractive in the market. As was asserted by provider P7, *"it's basically in the vendors' interest not to be defined!"* This may be for the CSP's good, but in my view it causes unnecessary confusion for clients.

What was surprising was that I could not stop myself from reflecting on the debate between CC and IS/IT outsourcing in the literature and the professional world.

The literature reported on comparisons made between CC and IS/IT outsourcing; from these, it appears that there are two key points that distinguish them from each other; scope and ownership (Schneider & Sunyaev 2014). These distinguishing points are applicable to public CC services; however, if we consider private clouds, we again drift towards IS/IT outsourcing.

In terms of scope, the literature has regarded CC as standardized software and infrastructures, while IS/IT outsourcing services have been seen as custom-tailored and covering hardware, software, people, and processes (Schneider & Sunyaev 2014). Public clouds are standardized, while private clouds are customized (Leavitt 2013). I add to this, the view of one of my informants, a security professional known by the code P16. His view was that outsourcing staff on-site of the client organization constitutes a private cloud. To me, this implies that people are also within the scope of CC!

In terms of the ownership, IT resources in public clouds are totally owned by the provider and its sub-providers, while in IS/IT outsourcing, IT resources are owned either partially or totally by the client or totally by the provider (Schneider & Sunyaev 2014). On the other hand, NIST considered private clouds as a CC deployment model where the IT resources are owned either totally or partially by the client, or totally by the provider (Mell & Grance 2011). The majority of my informants explained that there are two forms of private clouds; in one form, the client organization implements its own cloud and eliminates the dependency on external CSPs, whilst in the other form, the client organization makes sole use of the resources of a public datacenter without sharing them with other tenants, particularly other organizations.

As a whole, therefore, my interpretations lead me to view IS/IT outsourcing as a professional or scientific name and CC as a business name. Thus, I conclude that both names mean the same thing after all. I make no claims for a particular definition to be taken up by practitioners or researchers; rather, I claim that, as an interpretive

researcher, I create my own view of reality regarding the debate between CC and IS/IT outsourcing in an attempt to analyze the literature and the interpretations of my informants. This strongly indicates that CC is a socially constructed phenomenon that is viewed differently by different people.

References

Abokhodair, N. et al., 2012. Heading for the Clouds? Implications for Cloud Computing Adopters. In *Proceedings of the 18th Americas Conference on Information Systems (AMCIS 2012)*.

Abou El-Seoud, M.S. et al., 2013. Implementation of Web-Based Education in Egypt through Cloud Computing Technologies and Its Effect on Higher Education. *Higher Education Studies*, 3(3), pp.62–76.

Abrahamson, E., 1996. Management Fashion. *Academy of Management Review*, 21(1), pp.254–285.

Ågerfalk, P.J., 2014. Insufficient Theoretical Contribution: A Conclusive Rationale for Rejection? *European Journal of Information Systems*, 23, pp.593–599.

Akins, R.B., Tolson, H. & Cole, B.R., 2005. Stability of Response Characteristics of a Delphi Panel: Application of Bootstrap Data Expansion. *BMC Medical Research Methodology*, 5(37), pp.1–12.

Alshamaila, Y. & Papagiannidis, S., 2013. Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework. *Journal of Enterprise Information Management*, 26(3), pp.250–275.

Altaf, F. & Schuff, D., 2010. Taking a Flexible Approach to ASPs. *Communications of the ACM*, 53(2), pp.139–143.

Amant, K. St., 2009. *IT Outsourcing: Concepts, Methodologies, Tools, and Applications*, IGI Global.

Andriole, S.J., 2012. Seven Indisputable Technology Trends That Will Define 2015. *Communications of the Association for Information Systems*, 30(1), pp.61–72.

Andriole, S.J., 2015. Who owns IT? *Communications of the ACM*, 58(3), pp.50–57.

Ang, S. & Cummings, L.L., 1997. Strategic Response to Institutional Influences on Information Systems Outsourcing. *Organization Science*, 8(3), pp.235–256.

Anthes, G., 2010. Security in the Cloud. *Communications of the ACM*, 53(11), pp.16–18.

Armbrust, B. et al., 2010. A View of Cloud Computing. *Communications of The ACM*, 53(2), pp.50–58.

Armbrust, M. et al., 2009. Above the Clouds : A Berkeley View of Cloud Computing. , pp.7–13.

Arthur, C., 2011. Egypt Cuts off Internet Access. *The Guardian*. Available at: http://www.theguardian.com/technology/2011/jan/28/egypt-cuts-off-internet-access.

Avgerou, C., 2010. Discourses on ICT and Development. *Information Technologies and International Development*, 6(3), pp.1–18.

Avgerou, C., 2000. IT and Organizational Change: An Institutionalist Perspective. *Information Technology & People*, 13(4), pp.234–262.

Avram, M.G., 2014. Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, 12, pp.529–534.

Badger, L. et al., 2011. US Government Cloud Computing Technology Roadmap Volume I Release 1 . 0 (Draft) High-Priority Requirements to Further USG Agency Cloud. , pp.1–32.

Bakir, A. & Todorovic, M., 2010. A Hermeneutic Reading into "What Strategy is": Ambiguous Means-End Relationship. *Qualitative Report*, 15(5), pp.1037–1057.

Barley, S.R. & Tolbert, P.S., 1997. Institutionalization and Structuration: Studying the Links between Action and Institution. *Organization Studies*, 18(1), pp.93–117.

Barrett, M. et al., 2015. Service Innovation in the Digital Age: Key Contributions and Future Directions. *MIS Quartely*, 39(1), pp.135–154.

Benaroch, M., Dai, Q. & Kauffman, R.J., 2010. Should We Go Our Own Way? Backsourcing Flexibility in IT Services Contracts. *Journal of Management Information Systems*, 26(4), pp.317–358.

Benders, J., Batenburg, R. & van der Blonk, H., 2006. Sticking to Standards; Technical and Other Isomorphic Pressures in Deploying ERP-Systems. *Information & Management*, 43(2), pp.194–203.

Benlian, A., Koufaris, M. & Hess, T., 2011. Service Quality in Software-as-a-Service: Developing the SaaS-Qual Measure and Examining Its Role in Usage Continuance. *Journal of Management Information Systems*, 28(3), pp.85–126.

Bharadwaj, S.S. & Lal, P., 2012. Exploring the Impact of Cloud Computing Adoption on Organizational Flexibility: A Client Perspective. In *Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management*.

Bhat, J.M., 2013. Adoption of Cloud Computing by SMEs in India: A study of the Institutional Factors. In *Proceedings of the 19th Americas Conference on Information Systems*.

Bilbao-Osorio, B. et al., 2013. *The Networked Readiness Index 2013 : Benchmarking ICT Uptake and Support for Growth and Jobs in a Hyperconnected World*, World Economic Forum. Available at: http://www3.weforum.org/docs/GITR/2013/GITR_Chapter1.1_2013.pdf.

Bjorck, F., 2004. Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations. In *Proceedings of the 37th Hawaii International Conference on Systems Sciences*.

Borgman, H.P. et al., 2013. Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. In *Proceedings of the 46th Hawaii International Conference on System Sciences*.

Brian, O. et al., 2012. SATW White Paper: Cloud Computing. , pp.11–51. Available at: http://www.satw.ch/organisation/tpf/tpf_ict/box_feeder/2013-02-06_SATW_White_Paper_Cloud_Computing_EN.pdf.

Broadbent, M., Weill, P. & Neo, B.S., 1999. Strategic context and patterns of IT infrastructure capability. *The Journal of Strategic Information Systems*, 8(2), pp.157–187.

vom Brocke, J. et al., 2009. Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In *Proceedings of the 17th European Conference on Information Systems*.

Brynjolfsson, E., Hofmann, P. & Jordan, J., 2010. Cloud Computing and Electricity: Beyond the Utility Model. *Communications of the ACM*, 53(5), pp.32–34.

Bygstad, B. & Munkvold, B.E., 2010. Exploring the Role of Informants in Interpretive Case Study Research in IS. *Journal of Information Technology*, 26(1), pp.32–45.

Campbell-Kelly, M., 2009. Historical Reflections: The Rise, Fall, and Resurrection of Software as a Service. *Communications of the ACM*, 52(5), pp.28–30.

Cavaye, A.L.M., 1996. Case Study Research: A Multifaceted Research Approach for IS. *Information Systems Journal*, 6(3), pp.227–242.

Cegielski, C.G. et al., 2012. Adoption of Cloud Computing Technologies in Supply Chains: An Organizational Information Processing Theory Approach. *International Journal of Logistics Management*, 23(2), pp.184–211.

Chatterjee, D., Grewal, R. & Sambamurthy, V., 2002. Shaping Up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies. *MIS Quarterly*, 26(2), pp.65–89.

Checkland, P. & Holwell, S., 1999. Information, Systems and Information Systems: Making Sense of the Field. *The Journal of the Operational Research Society*, 50(5), pp.554–557.

Chen, P. & Wu, S., 2012. The Impact and Implications of On-Demand Services on Market Structure. *Information Systems Research*, 24(3), pp.1–18.

Chong, A.Y.-L. & Ooi, K.-B., 2008. Adoption of Interorganizational System Standards in Supply Chains: An Empirical Analysis of RosettaNet Standards. *Industrial Management & Data Systems*, 108(4), pp.529–547.

Cisco, 2013. *Cisco Global Cloud Index Supplement: Cloud Readiness Regional Details*, Available at: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/CloudIndex_Supplement.pdf.

Clemons, E.K. & Chen, Y., 2011. Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing. In *Proceedings of the 44th Hawaii International Conference on System Sciences*.

Cloud Security Alliance, 2013. *CSA Survey on NSA/PRISM*, Available at: https://cloudsecurityalliance.org/research/surveys/#_past.

Cordella, A. & Willcocks, L., 2012. Government Policy, Public value and IT Outsourcing: The Strategic Case of ASPIRE. *The Journal of Strategic Information Systems*, 21(4), pp.295–307.

Creeger, M., 2008. CTO Roundtable on Virtualization. *Communications of The ACM*, 51(11), pp.47–53.

CSA, 2009. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, Available at: https://cloudsecurityalliance.org/csaguide.pdf.

Currie, W., 2009. Contextualising the IT Artefact: Towards a Wider Research Agenda for IS Using Institutional Theory. *Information Technology & People*, 22(1), pp.63–77.

Currie, W. & Seltsikas, P., 2001. Exploring the Supply-Side of IT Outsourcing: Evaluating the Emerging Role of Application Service Providers. *European Journal of Information Systems*, 10(3), pp.123–134.

Currie, W.L., 2004. The Organizing Vision of Application Service Provision: a Process-Oriented Analysis. *Information and Organization*, 14(4), pp.237–267.

Currie, W.L. & Guah, M.W., 2007. Conflicting Institutional Logics: A National Programme for IT in the Organisational Field of Healthcare. *Journal of Information Technology*, 22(3), pp.235–247. Available at: http://www.palgrave-journals.com/doifinder/10.1057/palgrave.jit.2000102 [Accessed March 9, 2013].

Currie, W.L. & Parikh, M.A., 2006. Value Creation in Web Services: An Integrative Model. *The Journal of Strategic Information Systems*, 15(2), pp.153–174.

Cusumano, M., 2010. Technology Strategy and Management: Cloud computing and SaaS as New Computing Platforms. *Communications of the ACM*, 53(4), pp.27–29.

Dalkey, N.C., 1972. The Delphi Method: An Experimental Study of Group Opinion. In N. C. Dalkey, ed. *Studies in the quality of life: Delphi and decision-making*. Lexington Books, p. 161.

Darke, P., Shanks, G. & Broadbent, M., 1998. Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism. *Information Systems Journal*, 8(4), pp.273–289.

Datatilsynet, 2012. Use of Cloud Computing Services. *Datatilsynet*. Available at: https://www.datatilsynet.no/English/Publications/cloud-computing/.

Day, J. & Bobeva, M., 2005. A Generic Toolkit for the Successful Management of Delphi Studies. *The Electronic Journal of Business Research Methodology*, 3(2), pp.103–116.

Deephouse, D.L. & Suchman, M., 2008. Legitimacy in Organizational Institutionalism. In R. Greenwood et al., eds. *The SAGE Handbook of Organizational Institutionalism*. Thousand Oaks: SAGE Publications Ltd, pp. 49–77.

Denzin, N.K., 1978. *The Research Act* 2d ed., New York: McGraw-Hill.

Desai, B. et al., 2003. Market Entry Strategies of Application Service Providers: Identifying Strategic Differentiation. In *Proceedings of the 36th Hawaii International Conference on System Sciences*.

Desai, D., 2013. Beyond location: Data Security in the 21st Century. *Communications of the ACM*, 56(1), pp.34–36.

Devoteam daVinci, 2011. *Felles IKT-utvikling i kommunal sektor*, Available at: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Davinci_Felles_IKT-

utvikling_kommunal_sektor.pdf.

Dibbern, J. et al., 2004. Information Systems Outsourcing: A Survey and Analysis of the Literature. *ACM SIGMIS Database*, 35(4), pp.6–102.

Dibbern, J., Chin, W. & Heinzl, A., 2012. Systemic Determinants of the Information Systems Outsourcing Decision: A Comparative Study of German and United States Firms. *Journal of the Association for Information Systems*, 13(6), pp.466–497.

Diebold, F.X., Doherty, N.A. & Herring, R.J., 2010. *The Known, the Unknown, and the Unknowable in Financial Risk Management: Measurement and Theory Advancing Practice*, Princeton University Press.

DiMaggio, P. & Powell, W., 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48(2), pp.147–160.

Donnelly, C., 2015. Research Highlights Security Risk Posed by Cloud "Super" Users. *ComputerWeekly.com*. Available at: http://www.computerweekly.com/news/4500252395/Research-highlights-security-risk-posed-by-cloud-super-users.

Dowling, J. & Pfeffer, J., 1975. Organizational Legitimacy: Social Values and Organizational Behavior. *The Pacific Sociological Review*, 18(1), pp.122–136.

Dubey, A. & Wagle, D., 2007. Delivering software as a service. *The McKinsey Quarterly*, pp.1–12.

Duncan, N.B., 1995. Capturing Flexibility of Information Technology Infrastructure: A study of Resource Characteristics and Their Measure. *Journal of Management Information Systems*, 12(2), pp.37–57.

Durkee, D., 2010. Why Cloud Computing Will Never Be Free. *Communications of the ACM*, 53(5), pp.62–69.

Dutta, S., Bilbao-Osorio, B. & Geiger, T., 2012. *The Networked Readiness Index 2012: Benchmarking ICT Progress and Impacts for the Next Decade*, Available at: http://www3.weforum.org/docs/GITR/2012/GITR_Chapter1.1_2012.pdf.

Dutta, S., Geiger, T. & Lanvin, B., 2015. *The Global Information Technology Report 2015: ICTs for Inclusive Growth*, Available at: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf.

Dutta, S. & Mia, I., 2011. *The Global Information Technology Report 2010–2011*, Available at: http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf.

Earl, M.J., 1996. The Risks of Outsourcing IT. *MIT Sloan Management Review*. Available at: http://sloanreview.mit.edu/article/the-risks-of-outsourcing-it/.

Eaton, B. et al., 2014. Achieving Payoffs from an Industry Cloud Ecosystem at BankID. *MIS Quarterly Executive*, 13(4), pp.223–235.

Eisenhardt, K.M., 1989. Building Theories from Case Study Research. *The Academy of Management Review*, 14(4), pp.532–550.

El-Gazzar, R.F., 2014. A Literature Review on Cloud Computing Adoption Issues in Enterprises. In *IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014*. Springer Berlin Heidelberg, pp. 214–242.

eMarketing Egypt, 2013. *Facebook in Egypt: E-Marketing Insights*, Available at: http://www.emarketing-egypt.com/facebook-egypt-e-marketing-insights-2013-update-0.

ENISA, 2014. Annex Good Practice Guide for securely deploying Governmental Clouds.

Ernst&Young, 2012. *Ready for Takeoff: Preparing for Your Jurney into the Cloud*, Available at: http://assets-production.govstore.service.gov.uk/Giii Attachments/ERNST & YOUNG LLP/Bids/Ready for take-off.pdf.

Espadanal, M. & Oliveira, T., 2012. Cloud Computing Adoption by Firms. In *Proceedings of the*

Mediterranean Conference on Information Systems.

Etro, F., 2009. The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe. *Review of Business and Economics*, 54(2), pp.179–208.

Franklin, K. & Hart, J., 2007. Idea Generation and Exploration: Benefits and Limitations of the Policy Delphi Research Method. *Innovative Higher Education*, 31(4), pp.237–246.

Frelle-Petersen, L. et al., 2012. Nordic Public Sector Cloud Computing – A Discussion Paper. , pp.1–62.

Galliers, R.D. & Land, F.F., 1987. Choosing Systems Appropriate Research Information Methodologies. *Communications of the ACM*, 30(11), pp.900–902.

Gallivan, M. & Oh, W., 1999. Analyzing IT Outsourcing Relationships as Alliances Among Multiple Clients and Vendors. In *Proceedings of the 32nd Hawaii International Conference on System Sciences*.

Garrison, G., Kim, S. & Wakefield, R.L., 2012. Success Factors for Deploying Cloud Computing. *Communications of the ACM*, 55(9), pp.62–68.

Geertz, C., 1973. *The Interpretation of Cultures*, New York: Basic Books.

Glaser, B.G. & Strauss, A.L., 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine de Gruyter.

Gonzalez, R. & Dahanayake, A., 2007. A Concept Map of Information Systems Research Approaches. In *Proceedings of the IRMA International Conference*.

Gonzalez, R., Gasco, J. & Llopis, J., 2006. Information Systems Outsourcing: A Literature Analysis. *Information & Management*, 43(7), pp.821–834.

Goo, J. et al., 2009. The Role of Service Level Agreements in Relational Management of Information Technology Outsourcing: An Empirical Study. *MIS Quarterly*, 33(1), pp.119–145.

Gordon, T.J., 1994. The Delphi Method. *Futures Research Methodology*, 2.

Gould, J., 2012. Interview with the Norwegian Data Protection Commissioner. *SafeGov.org*. Available at: http://safegov.org/2012/11/23/interview-with-the-norwegian-data-protection-commissioner.

Greengard, S., 2010. Cloud Computing and Developing Nations. *Communications of the ACM*, 53(5), pp.18–20.

Gregor, S., 2006. The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3), pp.611–642.

Grover, V., Cheon, M. & Teng, J., 1996. The Effect of Service Quality and Partnership on the Outsourcing of Information Systems Functions. *Journal of Management Information Systems*, 12(4), pp.89–116.

Gupta, P., Seetharaman, A. & Raj, J.R., 2013. The Usage and Adoption of Cloud Computing by Small and Medium Businesses. *International Journal of Information Management*, 33(5), pp.861–874.

Haeberlen, T., Liveri, D. & Lakka, M., 2013. Good Practice Guide for Securely Deploying Governmental Clouds. , pp.1–46.

Halperin, S. & Heath, O., 2012. *Political Research: Methods and Practical Skills*, OUP Oxford.

Hana, M.A., 2013. E-Government Cloud Computing Proposed Model: Egyptian E-Government Cloud Computing. In *The International Conference on Advances in Computing, Communications and Informatics*.

Harlow, E., 2010. Contribution, Theoretical. In A. Mills, G. Durepos, & E. Wiebe, eds. *Encyclopedia of Case Study Research*. Thousand Oaks, CA: SAGE Publications, Inc., pp. 237–239.

Heart, T., 2010. Who is Out There ? Exploring the Effects of Trust and Perceived Risk on Saas Adoption Intentions. *The DATA BASE for Advances in Information Systems*, 41(3), pp.49–68.

Heidegger, M., 2005. *Introduction to Phenomenological Research*, Indiana University Press.

Heikkilä, J.-P., 2013. An Institutional Theory Perspective on e-HRM's Strategic Potential in MNC Subsidiaries. *The Journal of Strategic Information Systems*, 22(3), pp.238–251.

Heiser, J. & Nicolett, M., 2008. *Assessing the Security Risks of Cloud Computing*, Available at: http://www.globalcloudbusiness.com/SharedFiles/Download.aspx?pageid=138&mid=220&fileid=12.

Herhalt, J. & Cochrane, K., 2012. Exploring the Cloud: A Global Study of Governments' Adoption of Cloud. , pp.1–44. Available at: http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/Exploring-the-Cloud.pdf.

Hirschheim, R., Heinzl, A. & Dibbern, J., 2007. *Information Systems Outsourcing: Enduring Themes, New Perspectives and Global Changes* Second Edi., NewYork: 2nd ed. Springer BerlinHeidelberg.

Hogan, M. et al., 2011. NIST Cloud Computing Standards Roadmap. , pp.1–76.

Hsu, C., Lee, J. & Straub, D., 2012. Institutional Influences on Information Systems Security Innovations. *Information Systems Research*, 23(3), pp.918–939.

Hsu, C. & Sandford, B.A., 2007. The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research & Evaluation*, 12(10), pp.1–8.

Hu, Q., Saunders, C. & Gebelt, M., 1997. Research Report: Diffusion of Information Systems Outsourcing: A Reevaluation of Influence Sources. *Information Systems Research*, 8(3), pp.288–301.

Hustad, E. & Olsen, D.H., 2012. Adoption of Cloud Computing: A Study of Enablers and Inhibitors in a Norwegian Context. In *Proceedings of the 9th International Conference on Enterprise Systems, Accounting and Logistics*.

Huyskens, C. & Loebbecke, C., 2006. Determinants of Netsourcing : An Empirical Evaluation. In *Proceedings of Americas Conference on Information Systems*.

Iden, J., Tessem, B. & Päivärinta, T., 2011. Problems in the interplay of development and IT operations in system development projects: A Delphi study of Norwegian IT experts. *Information and Software Technology*, 53(4), pp.394–406.

Information Economy Report, 2013. *Information Economy Report 2013: The Cloud Economy and Developing Countries*, Available at: http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.

Ismail, N., 2011. Cursing the Cloud (or) Controlling the Cloud? *Computer Law & Security Review*, 27(3), pp.250–257.

ITU, 2013. Measuring Information Society. , pp.1–254. Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

ITU, 2011. Measuring the Information Society. , pp.1–174. Available at: http://www.itu.int/ITU-D/ict/publications/idi/material/2011/MIS_2011_without_annex_5.pdf.

ITU, 2014. *Measuring the Information Society*, Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf.

ITU, 2012. *Measuring the Information Society*, Available at: http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2012.aspx.

ITU, 2015. *Measuring the Information Society Report 2015*, Available at: http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf.

Iyer, B. & Henderson, J.C., 2012. Business Value from Clouds: Learning from Users. *MIS Quarterly Executive*, 11(1), pp.51–60.

Iyer, B. & Henderson, J.C., 2010. Preparing for The Future: Understanding The Seven Capabilities of Cloud Computing. *MIS Quarterly Executive*, 9(2), pp.117–131.

Iyer, E.K. et al., 2013. Analysis of Dissatisfiers That Inhibit Cloud Computing Adoption Across

Multiple Customer Segments. In *Proceedings of the European Conference on Information Management & Evaluation*.

James, N., 2007. The Use of Email Interviewing as a Qualitative Method of Inquiry in Educational Research. *British Educational Research Journal*, 33(6), pp.963–976.

James, N. & Busher, H., 2006. Credibility, Authenticity and Voice: Dilemmas in Online Interviewing. *Qualitative Research*, 6(3), pp.403–420.

Jansen, W. a, 2011. Cloud Hooks: Security and Privacy Issues in Cloud Computing. In *Proceedings of the 44th Hawaii International Conference on System Sciences*.

Jayatilaka, B., Schwarz, A. & Hirschheim, R., 2003. Determinants of ASP Choice: An Integrated Perspective. *European Journal of Information Systems*, 12, pp.210–224.

Jensen, M. et al., 2011. Security Prospects Through Cloud Computing by Adopting Multiple Clouds. In *Proceedings of the 4th International Conference on Cloud Computing (CLOUD)*.

Jick, T.D., 1979. Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, 24, pp.602–611.

Jørgenrud, M., 2011. Narvik velger Google Apps. *digi.no*. Available at: http://www.digi.no/868991/narvik-velger-google-apps.

Kern, T., Kreijger, J. & Willcocks, L., 2002. Exploring ASP as Sourcing Strategy: Theoretical Perspectives, Propositions for Practice. *The Journal of Strategic Information Systems*, 11(2), pp.153–177.

Kern, T., Lacity, M.C. & Willcocks, L.P., 2002. An Overview of Netsourcing. In *Netsourcing: Renting Business Applications and Services Over a Network*. New Jersey: Financial Times (Prentice Hall), pp. 1–33.

Kern, T. & Willcocks, L., 2000. Exploring Information Technology Outsourcing Relationships: Theory and Practice. *The Journal of Strategic Information Systems*, 9(4), pp.321–350.

Kern, T., Willcocks, L.P. & Lacity, M.C., 2002. Application Service Provision : Risk Assessment and Mitigation. *MIS Quarterly Executive*, 1(2), pp.113–126.

Khan, S.A. & Lacity, M.C., 2014. Organizational Responsiveness to Anti-Offshoring Institutional Pressures. *The Journal of Strategic Information Systems*, 23(3), pp.190–209.

Kim, W. et al., 2009. Adoption Issues for Cloud Computing. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services*.

King, J.L. et al., 1994. Institutional Factors in Information Technology Innovation. *Information Systems Research*, 5(2), pp.139–169.

Klein, H. & Myers, M., 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, 23(1), pp.67–93.

Kotsovinos, E., 2011. Virtualization: Blessing or Curse? *Communications of the ACM*, 54(1), pp.61–65.

Koutsoukis, N.-S. & Mitra, G., 2003. *Decision Modelling and Information Systems: The Information Value Chain*, Springer Science & Business Media.

Kristiansen, T., 2011. Strong Growth in Cloud Computing in Norway. *Reuters*. Available at: http://www.reuters.com/article/2011/09/07/idUS46774+07-Sep-2011+HUG20110907.

Kshetri, N., 2012. Cloud Computing in India. *IEEE IT Professional*, 14(5), pp.5–8.

Kshetri, N., 2013. Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution. *Telecommunications Policy*, 37(4-5), pp.372–386.

Kshetri, N. & Murugesan, S., 2013. Cloud Computing and EU Data Privacy Regulations. *Computer*, 46(3), pp.86–89.

Kushida, K.E., Murray, J. & Zysman, J., 2011. Diffusing the Cloud: Cloud Computing and

Implications for Public Policy. *Journal of Industry, Competition and Trade*, 11(3), pp.209–237.

Lacity, M., Hirschheim, R. & Willcocks, L., 1994. Realizing Outsourcing Expectations Incredible Expectations, Credible Outcomes. *Information Systems Management*, 11(4), pp.7–18.

Lacity, M. & Willcocks, L., 1998. An Empirical Investigation of Information Technology Sourcing Practices: Lessons from Experience. *MIS quarterly*, 22(3), pp.363–408.

Lacity, M., Willcocks, L. & Feeny, D., 1996. The Value of Selective IT Sourcing. *Sloan Management Review*, pp.13–25.

Lacity, M.C. et al., 2010. A Review of the IT Outsourcing Empirical Literature and Future Research Directions. *Journal of Information Technology*, 25(4), pp.395–433.

Lacity, M.C. & Hirschheim, R., 1995. Benchmarking as a Strategy for Managing Conflicting Stakeholder Perceptions of Information Systems. *The Journal of Strategic Information Systems*, 4(2), pp.165–185.

Lacity, M.C. & Hirschheim, R.A., 1993. *Information Systems Outsourcing: Myths, Metaphors, and Realities*, John Wiley.

Lacity, M.C., Khan, S.A. & Willcocks, L.P., 2009. A Review of the IT Outsourcing Literature: Insights for Practice. *The Journal of Strategic Information Systems*, 18(3), pp.130–146.

Lacity, M.C. & Reynolds, P., 2014. Cloud Services Practices for Small and Medium-Sized Enterprises. *MIS Quarterly Executive*, 13(1), pp.31–44.

Lacity, M.C., Willcocks, L.P. & Khan, S., 2011. Beyond Transaction Cost Economics: Towards an endogenous theory of Information Technology Outsourcing. *The Journal of Strategic Information Systems*, 20(2), pp.139–157.

Langley, A., 1999. Strategies for Theorizing from Process Data. *Academy of Management review*, 24(4), pp.691–710.

Lango, J., 2014. Toward Software-Defined SLAs. *Communications of the ACM*, 57(1), pp.54–60.

Lansing, J., Schneider, S. & Sunyaev, A., 2013. Cloud Service Certifications: Measuring Consumers' Preferences For Assurances. In *Proceedings of the 21st European Conference on Information Systems*.

Leavitt, N., 2013. Hybrid Clouds Move to the Forefront. *Computer*, 46(5), pp.15–18.

Lee, A. & Baskerville, R., 2003. Generalizing Generalizability in Information Systems Research. *Information Systems Research*, 14(3), pp.221–243.

Lee, J. et al., 2003. IT Outsourcing Evolution: Past, Present, and Future. *Communications of the ACM*, 46(5), pp.84–89.

Lee, J. & Kim, Y., 1999. Effect of Partnership Quality on IS Outsourcing Success: Conceptual Framework and Empirical Validation. *Journal of Management Information Systems*, 15(4), pp.29–61.

Leimeister, S., 2010. *IT Outsourcing Governance: Client Types and Their Management Strategies*, Springer Science & Business Media.

Levina, N. & Ross, J., 2003. From the Vendor's Perspective: Exploring the Value Proposition in Information Technology Outsourcing. *MIS quarterly*, 27(3), pp.331–364.

Levy, Y. & Ellis, T.J., 2006. A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science Journal*, 9, pp.181–212.

Li, M. et al., 2012. Drivers for Strategic Choice of Cloud Computing as Online Service in SMEs. In *Proceedings of the 33rd International Conference on Information Systems*.

Lian, J.-W., Yen, D.C. & Wang, Y.-T., 2014. An Exploratory Study to Understand the Critical Factors Affecting the Decision to Adopt Cloud Computing in Taiwan Hospital. *International Journal of Information Management*, 34(1), pp.28–36.

Liang, H. et al., 2007. Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS quarterly*, 31(1), pp.59–87.

Lin, A. & Chen, N., 2012. Cloud computing as an innovation : Percepetion, attitude, and adoption. *International Journal of Information Management*, 32(2012), pp.533–540.

Lin, A. & Chen, N.-C., 2012. Cloud Computing as an Innovation: Perception, Attitude, and Adoption. *International Journal of Information Management*, 32(6), pp.533–540.

Linstone, H. & Turoff, M., 1975. *The Delphi Method: Techniques and Applications*, Reading, MA: Addison-Wesley.

Linthicum, D., 2013. Cloud Adoption's Tipping Point Has Arrived. *InfoWorld*. Available at: http://www.infoworld.com/article/2611402/cloud-computing/cloud-adoption-s-tipping-point-has-arrived.html.

Linthicum, D.S., 2010. *Praise for Cloud Computing and SOA Convergence in Your Enterprise*, Pearson Education.

Loebbecke, C., Thomas, B. & Ullrich, T., 2012. Assessing Cloud Readiness at Continental AG. *MIS Quarterly Executive*, 11(1), pp.11–22.

Loh, L. & Venkatraman, N., 1992a. Determinants of Information Technology Outsourcing: A Cross-Sectional Analysis. *Journal of Management Information Systems*, 9(1), pp.7–24.

Loh, L. & Venkatraman, N., 1992b. Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect. *Information Systems Research*, 3(4), pp.334–358.

Loh, P., 2005. *Global IT Outsourcing: Key Issues & Trends*, Knowledgeworks Consultants.

Low, C., Chen, Y. & Wu, M., 2011. Understanding the Determinants of Cloud Computing Adoption. *Industrial Management & Data Systems*, 111(7), pp.1006–1023.

Luoma, E. & Nyberg, T., 2011. Four Scenarios for Adoption of Cloud Computing in China. In *Proceedings of the European Conference on Information Systems*.

Malladi, S. & Krishnan, M.S., 2012. Cloud Computing Adoption and its Implications for CIO Strategic Focus – An Empirical Analysis. In *Proceedings of the 33rd International Conference on Information Systems*.

Marshall, C. & Rossman, G.B., 1989. *Designing Qualitative Research* Fourth Edi., London: Sage.

Marston, S. et al., 2011. Cloud computing — The Business Perspective. *Decision Support Systems*, 51(1), pp.176–189.

Mathew, S.K. & Chen, Y., 2013. Achieving Offshore Software Development Success: An Empirical Analysis of Risk Mitigation through Relational Norms. *The Journal of Strategic Information Systems*, 22(4), pp.298–314.

Mcgeogh, B.T. & Donnellan, B., 2013. Factors That Affect the Adoption of Cloud Computing for an Enterprise: A Case Study of Cloud Adoption Within Intel Corporation. In *Proceedings of the 21st European Conference on Information Systems*.

MCIT, 2014a. *ICT Indicators in Brief*, Available at: http://mcit.gov.eg/Upcont/Documents/Publications_2422014000_EN_ICTIndicators_in_Brief_Jan2014.pdf.

MCIT, 2013. *MCIT Yearbook 2013*, Available at: http://www.mcit.gov.eg/Upcont/Documents/Yearbook2013_Final.pdf.

MCIT, 2014b. The Egyptian Government Cloud (EG-Cloud) Strategy. , pp.1–27. Available at: http://www.mcit.gov.eg/Upcont/Documents/EG-Cloud-Strategy-Final31-08-2014_final.pdf.

Meho, L., 2006. E-Mail Interviewing in Qualitative Research: A Methodological Discussion. *Journal of the American Society for Information Science and Technology*, 57(10), pp.1284–1295.

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing: Recommendations of the

National Institute of Standards and Technology. , pp.1–7.

Messerschmidt, C.M. & Hinz, O., 2013. Explaining the Adoption of Grid Computing: An Integrated Institutional Theory and Organizational Capability Approach. *The Journal of Strategic Information Systems*, 22(2), pp.137–156.

Mignerat, M. & Rivard, S., 2009. Positioning the Institutional Perspective in Information Systems Research. *Journal of Information Technology*, 24(4), pp.369–391.

Miles, M. & Huberman, A., 1984a. Drawing Valid Meaning from Qualitative Data: Toward a Shared Craft. *Educational Researcher*, 13(5), pp.20–30.

Miles, M. & Huberman, A., 1984b. *Qualitative Data Analysis: A Sourcebook of New Methods*,

Miles, M.B. & Huberman, A.M., 1994. *Qualitative Data Analysis: An Expanded Sourcebook*, SAGE Publications.

Mingers, J., 2001. Combining IS research methods: towards a pluralist methodology. *Information systems research*, 12(3), pp.240–259.

Ministry of Local Government and Modernization, 2013. Digital Agenda for Norway: ICT for Growth and Value Creation. *Ministry of Local Government and Modernisation*, pp.1–117.

Misra, S.C. & Mondal, A., 2011. Identification of a Company's Suitability for the Adoption of Cloud Computing and Modelling its Corresponding Return on Investment. *Mathematical and Computer Modelling*, 53(3-4), pp.504–521.

Morgan, L. & Conboy, K., 2013. Factors Affecting the Adoption of Cloud Computing: An Exploratory Study. In *Proceedings of the 21st European Conference on Information Systems*.

Morin, J.-H., Aubert, J. & Gateau, B., 2012. Towards Cloud Computing SLA Risk Management: Issues and Challenges. In *Proceedings of the 45th Hawaii International Conference on System Sciences*.

Myers, M.D. & Newman, M., 2007. The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization*, 17(1), pp.2–26.

Najjar, M.S. & Kettinger, W.J., 2013. Data Monetization: Lessons from a Retailer's Journey. *MIS Quarterly Executive*, 12(4), pp.21–32.

Nasir, U. & Niazi, M., 2011. Cloud Computing Adoption Assessment Model (CAAM). In *Proceedings of the 12th International Conference on Product Focused Software Development and Process Improvement*.

Nasr, A.A.O. & Galal-edeen, G.H., 2012. Proposed Development Model of e-Government to Appropriate Cloud Computing. *International Journal of Reviews in Computing*, 9(7), pp.1–7.

Nedbal, D. et al., 2014. OptiCloud: Development of a Private Cloud Infrastructure to Optimize Workload Placement Using Software Defined Networks Based on OpenStack. In *Proceedings of the 20th Americas Conference on Information Systems*.

Neumann, P.G., 2014. Risks and Myths of Cloud Computing and Cloud Storage. *Communications of the ACM*, 57(10), pp.25–27.

Nkhoma, M.Z., Dang, D.P.T. & Souza-daw, A. De, 2013. Contributing Factors of Cloud Computing Adoption: A Technology- Organisation-Environment Framework Approach. In *Proceedings of the European Conference on Information Management & Evaluation*.

NTT Communications, 2015. *Cloud Reality Check 2015*, Available at: http://info.us.ntt.com/rs/nttamericainc/images/WP-Cloud-Reality-Check.pdf.

NTT Communications, 2014. *NSA After-Shocks: How Snowden has Changed ICT Decision-Makers' Approach to the Cloud*, Available at: http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf.

NTT Europe, 2013. *Growing Pains in the Cloud: 300 CIOs Express their Views about Barriers to Cloud Adoption*,

Nuseibeh, H., 2011. Adoption of Cloud Computing in Organizations. In *Proceedings of the 17th Americas Conference on Information Systems*.

O'Donoghue, C., 2012. The Norwegian Data Protection Authority Holds off Ban, Permitting the Use of Cloud Computing Services by Norway Municipalities. *Global Regulatory Enforcement Law Blog*. Available at: http://www.globalregulatoryenforcementlawblog.com/2012/10/articles/data-security/the-norwegian-data-protection-authority-holds-off-ban-permitting-the-use-of-cloud-computing-services-by-norway-municipalities/.

Okoli, C. & Pawlowski, S.D., 2004. The Delphi Method as a Research Tool: An Example, Design Considerations and Applications. *Information & Management*, 42(1), pp.15–29.

Okoli, C. & Schabram, K., 2010. A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems*, 10(26), pp.1–49.

Oliver, C., 1991. Strategic Responses to Institutional Processes. *The Academy of Management Review*, 16(1), pp.145–179.

Olsen, T., 2015. Cloud Computing and Data Protection Compliance - Experiences from Norway. Available at: http://www.jus.uio.no/ifp/english/research/events/2015/cococloudthomasolsen.pdf.

Onwudebelu, U. & Chukuka, B., 2012. Will Adoption of Cloud Computing Put the Enterprise at Risk? In *Proceedings of the 4th International Conference on Adaptive Science & Technology*.

Opala, O.J. & Rahman, S. (Shawon) M., 2013. An Exploratory Analysis of the Influence of Information Security on the Adoption of Cloud Computing. In *Proceedings of the 2013 8th International Conference on System of Systems Engineering*.

Orlikowski, B.W.J. & Barley, S.R., 2001. Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS Quarterly*, 25(2), pp.145–165.

Orlikowski, W.J. & Baroudi, J.J., 1991. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, 2(1), pp.1–28.

Osman, F. et al., 2011. Egypt Revolution. *Blue Kaizen*, pp.4–9. Available at: http://www.bluekaizen.org/securitykaizen_mag/issue2/Security_Kaizen_2.pdf.

Owens, D., 2010. Securing Elasticity in The Cloud. *Communications of The ACM*, 53(8), pp.1–7.

Palinkas, L.A. et al., 2013. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), pp.533–544.

Paquette, S., Jaeger, P.T. & Wilson, S.C., 2010. Identifying the Security Risks Associated with Governmental Use of Cloud Computing. *Government Information Quarterly*, 27(3), pp.245–253.

Parakala, K. & Udhas, P., 2011. The Cloud Changing the Business Ecosystem. , pp.1–116. Available at: http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The_Cloud_Changing_the_Business_Ecosystem.pdf.

Patton, M.Q., 1990. *Qualitative Evaluation and Research Methods*,

Patton, M.Q., 2014. *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*, SAGE Publications.

Pfaller, R., Fiedler, M. & Picot, A., 2013. Rules Of Efficiency Or Legitimacy ? Antecedents Of It-Outsourcing - A Longitudinal Approach. In *Proceedings of the 21th European Conference on Information Systems*.

Pishdad, A. & Haider, A., 2013. ERP Institutionalization: Exploring the Influential Factors. *Journal of Enterprise Information Management*, 26(6), pp.642–660.

Powell, W.W. & DiMaggio, P.J., 1991. Introduction. In *The New Institutionalism in Organizational*

Analysis. pp. 1–38.

Rath, A. et al., 2012. Decision Points for Adoption Cloud Computing in Small, Medium Enterprises (SMEs). In *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions*.

Rawal, A., 2011. Adoption of Cloud Computing in India. *Journal of Technology Management for Growing Economies*, 2(2), pp.65–78.

Report Arab Social Media, 2013. Twitter in The Arab Region. Available at: http://www.arabsocialmediareport.com/Twitter/LineChart.aspx?&PriMenuID=18&CatID=25&mnu=Cat.

Rich, P., 2012. Inside the Black Box : Revealing the Process in Applying a Grounded Theory Analysis. *The Qualitative Report*, 17(25), pp.1–23.

RightScale, 2013. *State of the Cloud Report*, Available at: https://www.rightscale.com/pdf/rightscale-state-of-the-cloud-report-2013.pdf.

RightScale, 2014. *State of the Cloud Report*, Available at: http://assets.rightscale.com/uploads/pdfs/RightScale-2014-State-of-the-Cloud-Report.pdf.

Rivard, S. & Aubert, B.A., 2008. *Information Technology Outsourcing* S. Rivard & B. A. Aubert, eds., Armonk, New York: M.E. Sharpe.

Rogers, E.M., 1995. *Diffusion of Innovations* Fifth Edit., New York: Free Press.

Rogers, E.M., 2003. The Innovation-Decision Process. In *Diffusion of Innovations*. New York: Free Press.

Ryan, M.D., 2011. Cloud Computing Privacy Concerns on Our Doorstep. *Communications of the ACM*, 54(1), pp.36–38.

Sabherwal, R., 1999. The Role of Trust in Outsourced IS Development Projects. *Communications of the ACM*, 42(2), pp.80–86.

Salem, F. & Mourtada, R., 2012. *Social Media in the Arab World: Influencing Societal and Cultural Change?*, Available at: http://www.dimed.gouv.fr/sites/dimed.gouv.fr/files/asmr_-_social_media_in_the_arbian_world-influencing_societal_and_cultural_change_-_juillet_2012.pdf.

Saya, S., Pee, L.G. & Kankanhalli, A., 2010. The Impact of Institutional Influences on Perceived Technological Characteristics and Real Options in Cloud Computing Adoption. In *Proceedings of the 31st International Conference on Information Systems*.

Schacter, D.L. & Coyle, J.T., 1997. *Memory Distortion: How Minds, Brains, and Societies Reconstruct the Past* D. L. Schacter, ed., Harvard University Press.

Schmidt, R. et al., 2001. Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems*, 17(4), pp.5–36.

Schmidt, R.C., 1997. Managing Delphi Surveys Using Nonparametric Statistical Techniques. *Decision Sciences*, 28(3), pp.763–774.

Schneider, S. & Sunyaev, A., 2014. Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. *Journal of Information Technology*, pp.1–31.

Schwab, K. & Eide, E.B., 2014. *The Global Information Technology Report 2014 Rewards and Risks of Big Data* S. Dutta & B. Lanvin, eds., Available at: http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf.

Schwab, K. & Greenhill, R., 2012. *The Global Information Technology Report 2012: Living in a Hyperconnected World* S. Dutta & B. Bilbao-Osorio, eds., Available at: http://www3.weforum.org/docs/Global_IT_Report_2012.pdf.

Schwarz, A. et al., 2009. A Conjoint Approach to Understanding IT Application Services Outsourcing.

Journal of the Association for Information Systems, 10(10), pp.748–781.

Scott, W.R., 2004. Institutional Theory : Contributing to a Theoretical Research Program. In *Great Minds in Management: The Process of Theory Development,*. Oxford UK: Oxford University Press.

Scott, W.R., 2001. *Institutions and Organizations*, Sage.

Seddon, J.J.M. & Currie, W.L., 2013. Cloud computing and Trans-Border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance. *Health Policy and Technology*, 2(4), pp.229–241.

Seltsikas, P. & Currie, W.L., 2002. Evaluating the Application Service Provider (ASP) Business Model: The Challenge of Integration. In *Proceedings of the 35th Hawaii International Conference on System Sciences*.

Shahin, M., 2012. Egypt's ICT Lanscape: A Locomotive for Growth and Development. , pp.1–31.

Shin, J. et al., 2013. Strategic Management of Cloud Computing Services: Focusing on Consumer Adoption Behavior. *IEEE Transactions on Engineering Management*, 61(3), pp.1–9.

Smith, M.A. & Kumar, R.L., 2004. A theory of Application Service Provider (ASP) Use From a Client Perspective. *Information & Management*, 41(8), pp.977–1002.

Su, N., 2011. Emergence of Cloud Computing: An Institutional Innovation Perspective. In *Proceedings of the 32nd International Conference on Information Systems*.

Su, N. et al., 2009. Shared Services Transformation : Conceptualization and Valuation from the Perspective of Real Options. *Decision Sciences*, 40(3), pp.381–402.

Subramanian, B., 2012. The Disruptive Influence of Cloud Computing and its Implications for Adoption in the Pharmaceutical and Life Sciences Industry. *Journal of Medical Marketing: Device, Diagnostic and Pharmaceutical Marketing*, 12(3), pp.192–203.

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

Suddaby, R., 2010. Challenges for Institutional Theory. *Journal of Management Inquiry*, 19(1), pp.14–20.

Sultan, N., 2013. Cloud Computing: A Democratizing Force? *International Journal of Information Management*, 33(5), pp.810–815.

Sultan, N.A., 2011. Reaching for the "Cloud": How SMEs Can Manage. *International Journal of Information Management*, 31(3), pp.272–278.

Susarla, A. & Barua, A., 2011. Contracting Efficiency and New Firm Survival in Markets Enabled by Information Technology. *Information Systems Research*, 22(2), pp.306–324.

Susarla, A., Barua, A. & Whinston, A., 2003. Understanding the Service Component of Application Service Provision: An Empirical Analysis of Satisfaction with ASP Services. *MIS Quarterly*, 27(1), pp.91–123.

Swanson, E. & Ramiller, N., 1997. The Organizing Vision in Information Systems Innovation. *Organization Science*, 8(5), pp.458–474.

Swanson, E.B., 2010. Consultancies and Capabilities in Innovating with IT. *The Journal of Strategic Information Systems*, 19(1), pp.17–27.

Swanson, E.B., 1994. Information Systems Innovation among Organizations. *Management Science*, 40(9), pp.1069–1092.

Swanson, E.B. & Ramiller, N.C., 2004. Innonvating Mindfully with Information Technology. *MIS Quarterly*, 28(4), pp.553–583.

Tebboune, D.S., 2003. Application Service Provision: Origins and Development. *Business process management journal*, 9(6), pp.722–734.

Telenor, 2013. The Cloud Meets Fibre Optic Broadband. Available at: http://www.telenor.com/media/press-releases/2013/the-cloud-meets-fibre-optic-broadband/.

Thong, J.Y.L., 1999. An Integrated Model of Information Systems Adoption in Small Businesses. *Journal of Management Information Systems*, 15(4), pp.187–214.

Tjikongo, R. & Uys, W., 2013. The Viability of Cloud Computing Adoption in SMME's in Namibia. In *Proceedings of IST-Africa Conference*.

Toe, H.H., Wei, K.K. & Benbasat, I., 2003. Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective. *MIS Quarterly*, 27(1), pp.19–49.

Tolbert, P.S. & Zucker, L.G., 1996. The Institutionalization of Institutional Theory. In S. R. Clegg, C. Hardy, & W. R. Nord, eds. *Handbook of Organization Studies*. London: SAGE, pp. 175–190.

Tung, L. & Rieck, O., 2005. Adoption of Electronic Government Services Among Business Organizations in Singapore. *The Journal of Strategic Information Systems*, 14(4), pp.417–440.

Turoff, M., 1998. Alternative Futures for Distance Learning: The Force and the Darkside. *Online Journal of Distance Learning Administration*, 1(1).

UN, 2012. *Country Classification: World Economic Situation and Prospects 2012*, Available at: http://unctad.org/en/Docs/wesp2012_en.pdf.

UN, 2002. *Egypt Country Profile*, Available at: http://www.un.org/esa/agenda21/natlinfo/wssd/egypt.pdf.

Venters, W. & Whitley, E. a, 2012. A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology*, 27(3), pp.179–197.

Veum, H. & Nymoen, L.-O., 2012. Reply - Use of Microsoft Office 365 Cloud Computing Services - Municipality of Moss. , pp.1–10. Available at: http://www.datatilsynet.no/Global/english/12 0699 Datatilsynet-Moss kommune-en.pdf.

Veum, H. & Thoreid, R., 2012. Case Closed - New e-mail Solution for the Municipality of Narvik - Google Apps. , pp.1–18. Available at: https://www.datatilsynet.no/Global/english/12 0699 Datatilsynet-Narvik kommune-en.pdf.

Walsham, G., 2006. Doing Interpretive Research. *European Journal of Information Systems*, 15(3), pp.320–330.

Walsham, G., 1995. Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems*, 4, pp.74–81.

Wang, P., 2010. Chasing the Hottest IT: Effects of Information Technology Fashion on Organizations. *MIS Quartely*, 34(1), pp.63–85.

Ward, J.M., 2012. Information Systems Strategy: Quo Vadis? *The Journal of Strategic Information Systems*, 21(2), pp.165–171.

Webster, J. & Watson, R., 2002. Analysing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), pp.xiii–xxiii.

Weerakkody, V., Dwivedi, Y.K. & Irani, Z., 2009. The Diffusion and Use of Institutional Theory: A Cross-disciplinary Longitudinal Literature Survey. *Journal of Information Technology*, 24(4), pp.354–368.

Whitten, D. & Wakefield, R.L., 2006. Measuring Switching Costs in IT Outsourcing Services. *The Journal of Strategic Information Systems*, 15(3), pp.219–248.

Whittington, R., 2001. *What is Strategy - and Does it Matter?*, Cengage Learning EMEA.

Willcocks, L. & Lacity, M.C., 1997. The Sourcing and Outsourcing of IS: Shock of the New? In L. Willcocks & M. C. Lacity, eds. *Strategic sourcing of information systems: perspectives and practices*. Wiley, pp. 1–41.

Willcocks, L.P., Lacity, M.. & Kern, T., 1999. Risk Mitigation in IT Outsourcing Strategy Revisited: Longitudinal Case Research at LISA. *The Journal of Strategic Information Systems*, 8(3),

pp.285–314.

Williams, C., 2011. How Egypt Shut Down the Internet. *The Telegraph*. Available at: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

Wolfswinkel, J.F., Furtmueller, E. & Wilderom, C.P.M., 2011. Using Grounded Theory as a Method for Rigorously Reviewing Literature. *European Journal of Information Systems*, 22(1), pp.45–55.

Wooten, M. & Hoffman, A.J., 2008. Organizational Fields: Past, Present and Future. In R. Greenwood et al., eds. *The SAGE Handbook of Organizational Institutionalism*. Thousand Oaks: SAGE Publications Ltd.

Xin, M. & Levina, N., 2008. Software-as-a-Service Model: Elaborating Client-Side Adoption Factors. In *Proceedings of the 29th Conference on Information Systems*.

Yang, H. & Tate, M., 2012. A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 31(1), pp.35–60.

Yao, Y., Watson, E. & Khan, B. k., 2010. Application Service Providers: Market and Adoption Decisions. *Communications of the ACM*, 53(7), pp.113–117.

Yin, R.K., 2009. Designing Case Studies: Identifying Your Case (s) and Establishing the Logic of Your Case Study. In *Case Study Research: Design and Methods*. London: SAGE Publications, Incorporated, pp. 25–66.

Zielinski, D., 2009. Be Clear on Cloud Computing Contracts. *HR Magazine*, pp.63–65.

Appendix A: Research Publications

1. Paper1: El-Gazzar, R., & Wahid, F. (2013). An Analytical Framework to Understand the Adoption of Cloud Computing: An Institutional Theory Perspective. In *Proceedings of the International Conference on Cloud Security Management (ICCSM2013)* (pp. 91–98). Academic Conferences and Publishing International.
2. Paper2: El-Gazzar, R. F. (2014). A Literature Review on Cloud Computing Adoption Issues in Enterprises. In *IFIP WG 8.6 International Conference on Transfer and Diffusion of IT, TDIT 2014, Aalborg, Denmark, June 2-4, 2014* (pp. 214–242). Springer Berlin Heidelberg.
3. Paper3: El-Gazzar, R. F. (2015). The Start of a Journey to The Cloud in The Developing World : A Case Study of Egypt. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS 2015)* (pp. 4345–4354). doi:10.1109/HICSS.2015.520.
4. Paper4: El-Gazzar, R. F., & Wahid, F. (2015). Strategies for Cloud Computing: Insights from the Norwegian Public Sector. In *Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS 2015).*
5. Paper5: El-Gazzar, R. F., Hustad, E., & Olsen, D. H. (2016). Understanding Cloud Computing Adoption Issues: A Delphi Study Approach. (Accepted for publication in the Journal of Systems and Software). The article is currently in-press: http://www.sciencedirect.com/science/article/pii/S016412121630036X.

An Analytical Framework to Understand the Adoption of Cloud Computing: An Institutional Theory Perspective

Rania El-Gazzar[1] and Fathul Wahid[1,2]
[1]Department of Information Systems, University of Agder, Kristiansand, Norway
[2]Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
rania.f.el-gazzar@uia.no
fathul.wahid@uia.no

Abstract: Cloud computing (CC) offers a new information technology service model for organizations. In spite of its possible benefits, however, it also poses some serious concerns. Why do organizations adopt CC in spite of its potential risks? Based on several core concepts based on institutional theory, we propose an analytical framework to better understand the adoption of CC by organizations. We focus on the concepts of field-level changes, organizational fields, institutional isomorphism, and institutional strategic responses within the context of CC adoption. We identify a number of organizations that form the organizational field and bring about changes (i.e., CC providers, peer organizations, business partners, professional and industry associations, and regulators) that may trigger institutional pressures (i.e., coercive, normative, and mimetic) on the adopting organizations. We conclude by presenting possible strategic responses (i.e., acquiescence, compromise, avoidance, defiance, and manipulation) to address the institutional pressures related to CC adoption.

Keywords: cloud computing, institutional theory, adoption, organizational field, institutional isomorphism, strategic responses

1. Introduction

The concept of cloud computing (CC) has received considerable attention in academic and technical literature over the past several years (Timmermans et al. 2010; Yang & Tate 2012). The extant literature reports various benefits that CC may provide for organizations, including simplicity, cost efficiency, reduced demand for skilled labor, and scalability (Armbrust et al. 2010; Venters & Whitley 2012; Garrison et al. 2012). However, the literature also forewarns adopters to pay attention to potential risks associated with the implementation, management, and use of CC services (Marston et al. 2011).

Notwithstanding these potential risks, several sources indicate that the adoption of CC has been growing significantly (Catteddu 2010; Lee et al. 2011; CSA & ISACA 2012). CC offers a compelling solution for small- and medium-sized enterprises (SMEs) due to its low-entry barriers, both technical and financial, for using such sophisticated services. In contrast, large enterprises (LEs) possess surplus resources and can afford to implement an in-house information technology (IT) infrastructure (Weinhardt et al. 2009; Gordon et al. 2010; Son et al. 2011; Li et al. 2012). However, some questions regarding the use of CC have not been clearly addressed in the literature to date. For example, does CC leverage its promises to the adopters, what factors affect the decision to adopt or not to adopt CC, and do these factors affect the way the adopters manage the potential risks and/or exploit the promising benefits?

As a preliminary effort to address these issues, we propose an analytical framework to better understand the process of CC adoption by organizations. As the extant literature pays more attention to the benefits of CC than to its risks, we expect that the framework will be useful for answering the question of, *Why do organizations adopt CC in spite of its potential risks*?

To develop the framework for this study, we have relied on the concept of institutional theory, which is well-suited for gaining a better understanding of the various stages of the IT institutionalization process and the interactions between IT and the institution (Swanson & Ramiller 2004; Mignerat & Rivard 2009). In addition, institutional theory equips us with various concepts for better understanding the impact of internal and external factors on organizations that are engaged in IT-induced changes (Mignerat & Rivard 2009; Weerakkody et al. 2009). The theory is also able to capture the notion of "irrationality" in decision-making processes (Meyer & Rowan 1977; DiMaggio & Powell 1983; Mouritsen 1994), such as when an organization adopts CC to keep up with the industry hype and not just to reduce costs.

The remainder of the paper is structured as follows: In Section 2, we describe the concept of CC, along with its associated benefits and risks. The underlying concepts of institutional theory are presented in Section 3. In Section 4, we develop an analytical framework by connecting the institutional concepts supported with arguments from the extant literature. Section 5 ends the paper with conclusions and possible ways to use the framework in future research.

2. Cloud computing

The CC paradigm has emerged from previous distributed computing technologies such as grid computing and virtualization (Sultan 2011). CC is classified as a form of IT outsourcing through which shared IT resources are pooled in large external data centers and made accessible by users through the Internet (Venters & Whitley 2012). Commonly, CC is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance 2011, p. 2).

CC services are delivered by the provider to users via various models, such as Software as a Service (SaaS), Platform as a Service (PaaS), and/or Infrastructure as a Service (IaaS) (Mell & Grance 2011). The SaaS model provides Internet-based access to applications created by the CC provider. The PaaS model provides programming languages and tools supported by the CC provider via the Internet to develop and deploy user-created applications. The IaaS model provides computing resources (e.g., processing power, storage, and network).

Further, CC can be deployed in various forms, such as public, private, community, and hybrid clouds (Mell & Grance 2011). A public cloud infrastructure is accessible by the general public and is owned by the CC provider. A private cloud infrastructure is owned and managed by the user/organization. A community cloud is a private one shared by several organizations that have common concerns. The hybrid cloud infrastructure is a combination of two or more private, public, or community clouds that are linked together by standardized technology to ensure data and application portability. In addition to CC providers and users, there are "enablers" or "intermediaries" that manage the relationships between cloud providers and users and that facilitate CC adoption and use (Marston et al. 2011).

Regarding CC adoption, "there are significant technical, operational, and organizational issues which need to be tackled […] at the enterprise level" (Marston et al. 2011, p. 184). Hence, there are two views regarding the emergence of CC—optimistic and pessimistic. From an optimistic viewpoint, CC may bring economic, strategic, and technological benefits to organizations (Garrison et al. 2012). Organizations can increase their productivity and focus on their core business activities due to the decreased need to set-up in-house IT infrastructure, thus saving IT-related capital expenditures while achieving business agility (Ernst & Young 2011; Kepes 2011; Garrison et al. 2012). Since CC services are scalable, they adequately suit different users' needs and environments on a pay-as-you-go subscription basis (Durkee 2010; Mell & Grance 2011). Nevertheless, we cannot neglect the more pessimistic viewpoint that focuses on the potential risks and problems of CC adoption. Commonly identified CC risks are privacy (this includes control over the data, as well as trust, legal, and ethical issues), cultural differences at both corporate and geographical levels, and switching costs resulting from the vendor lock-in problem (Dillon et al. 2010; Ernst & Young 2011; Yang & Tate 2012). To comprehensively evaluate and understand CC adoption by organizations, it is important to look at both the benefits and risks of this process.

3. Theoretical basis

Institutional theory is rooted in the social sciences with contributions from various disciplines including economics, political science, organization science, and information systems (IS)/IT studies (Scott 2004; Currie 2009; Mignerat & Rivard 2009). Regarding IS/IT-related phenomena, it is argued that institutional theory has relevance to "understanding the impact of internal and external influences on organizations that are engaged in […] IT-induced change" (Weerakkody et al. 2009, p. 355). In the context of IS research, many studies have utilized institutional theory to "examine IS/IT-related phenomena exemplified in IT innovation, IS development and implementation, and IT adoption and use" (Mignerat & Rivard 2009, p. 1).

The rationale for choosing institutional theory to construct our analytical framework is twofold: It increases our understanding of "how institutions influence the design, use, and consequences of technologies, either within or across organizations" (Orlikowski & Barley 2001, p. 153) and it captures the notion of irrationality in decision-making through which organizational actors seek legitimacy more than efficiency (Avgerou 2000; Orlikowski & Barley 2001; Mignerat & Rivard 2009). This legitimacy is gained when these actors "accept and follow social norms unquestioningly, without any real reflection" (Tolbert & Zucker 1996, p. 176). In constructing the analytical framework, we focus on several core concepts that are germane to the understanding of CC adoption: field-level changes, isomorphic pressures, strategic responses, and institutional impacts. Each of these concepts is succinctly described below. The relationships among these concepts are depicted in Figure 1.

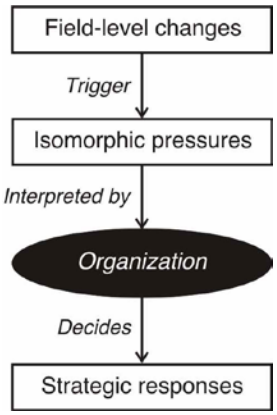


Figure 1: The core concepts

Field-level changes. To obtain acceptance and legitimacy, organizations are required to conform to a set of rules and requirements at the organizational field level (Wooten & Hoffman 2008). The organizational field is defined as "a community of organizations that partakes of a common meaning system and whose participants interact more frequently and fatefully with one another than with actors outside the field" (Scott 2001, p. 84). This may include government, critical exchange partners, sources of funding, professional and trade associations, special interest groups (e.g., industry level), and the general public (Scott 1991). Nonetheless, the concept of an organizational field has been dilated beyond geography and goals to encompass organizations that produce similar services or products (e.g., competitors), consumers, suppliers, and regulatory agencies (DiMaggio & Powell 1983). Changes at this organizational field level trigger various isomorphic pressures to organizations operating in that field.

Institutional isomorphism. At the field level, organizations confront powerful forces (i.e., isomorphic pressures) that cause them to become more similar to one another, thus achieving isomorphism (DiMaggio & Powell 1983). Institutional isomorphism is argued as "a useful tool for understanding the politics and ceremony that pervade much modern organizational life" (DiMaggio & Powell 1983, p. 150).

Institutional isomorphism manifests in three forms (DiMaggio & Powell 1983): *coercive, normative,* and *mimetic*. Coercive isomorphism results from both formal (e.g., regulations) and informal (e.g., culture) pressures exerted on organizations by their legal environment. Normative isomorphism results from pressures exerted by professional associations that define normative rules about organizational and professional behavior. Likewise, universities and professional training institutions produce individuals with similar orientations and educational backgrounds; for instance, an organization might decide to adopt cloud services because its managers learn that cost reduction is a good thing. Mimetic isomorphism results from uncertainties (e.g., goal ambiguity or poor awareness of organizational innovation); organizations are influenced by their competitors in the field and tend to imitate them, expecting similar success. These various isomorphic pressures force organizations to response accordingly and strategically.

Strategic responses. A key theme of institutional theory is that "an organization's survival requires it to conform to social norms of acceptable behavior" (Covaleski & Dirsmith 1988, p. 563). At the *organizational level*, organizations may enact five strategies expressed through tactics to cope with various isomorphic pressures in order to gain, maintain, or repair their legitimacy (Oliver 1991; Suchman 1995). While "early

adoption decisions of organizational innovations are commonly driven by a desire to improve performance" (DiMaggio & Powell 1983, p. 148), as innovations diffuse, the adoption decision becomes driven by the desire to achieve legitimacy rather than to improve performance (Meyer & Rowan 1977). Legitimacy is defined as the "congruence between the social values associated with or implied by [organizational] activities and the norms of acceptable behavior in the larger social system" (Dowling & Pfeffer 1975, p. 122).

These strategic responses are dependent on how organizations interpret the isomorphic pressures that they should conform to. According to Oliver (1991), organizations may (1) just conform to institutional norms through an *acquiescence* strategy, (2) balance themselves with their institutional environment through a *compromise* strategy when they confront a conflict between institutional norms and internal organizational objectives, (3) preclude the need for conformity to institutional norms through an *avoidance* strategy, (4) resist the institutional norms by using a *defiance* strategy, or (5) seek to import, influence, or control institutional constituents with a *manipulation* strategy. By relying on these concepts drawn from institutional theory, we build our analytical framework as follows.

4. Constructing an analytical framework

In constructing the analytical framework, we place the concepts of institutional theory into the context of CC adoption. In this conceptual paper, our arguments are more descriptive than normative. We examine the plausibility of the framework by bringing in relevant literature on the use of CC in specific and enterprise systems since our focus is on the adoption of CC at the organizational level.

Field-level changes. We start by identifying relevant organizations that form the organizational field. Field-level changes, such as the enactment of new government regulations, the ways of collaborating between business partners, and the advent of new CC services, trigger various isomorphic pressures. In the context of CC adoption, it is important to understand "how technologies are embedded in complex interdependent social, economic, and political networks, and how they are consequently shaped by such broader institutional influences" (Orlikowski & Barley 2001, p. 154). Based on our review of the extant literature, we identify the relevant organizations at the field level, which are summarized in Table 1.

Table 1: Organizations at the field level

Organization	Description	References
CC providers	Various forms of CC (SaaS, PaaS, and IaaS) offered by CC providers, along with their promised benefits and associated potential risks, affect CC adoption.	Armbrust et al. (2010)
Peer organizations	Organizations develop this trust through asking their peers about their perceptions of CC providers' capabilities and reputations.	Altaf & Schuff (2010) Heart (2010) Yao et al. (2010)
Business partners	Business partners (e.g., customers and suppliers) may affect the organization's decision to adopt CC services in order to keep on their partnership.	Li et al. (2012)
Professional and industry associations	Professional and industry associations may develop guidelines to facilitate CC adoption, as well as evaluation criteria to select appropriate CC providers.	Badger et al. (2011) Kshetri (2012)
Regulators	Regulators may enact obligations on CC providers to inform the adopting organizations about the protection of data security, privacy, and integrity. This is more important among government agencies.	Marston et al. (2011) Kshetri (2012)

Institutional isomorphism. As stated previously, various isomorphic pressures may be the result of changes at the field level. *Coercive* pressures may be exerted by other organizations through compulsory power such as parent organizations or trading partners with higher bargaining powers (Chong & Ooi 2008).

Other organizations may adopt CC because of their learning process, such as adhering to professional standards or observing earlier adopters. This process, which enables them to see potential benefits that may be harvested (Herhalt & Cochrane 2012), creates a *normative* isomorphic pressure. They assess and explore the value proposition of CC before making a decision.

Mimetic pressures may emerge from industry trends, the media, and consultants' influence (Benders et al. 2006). For example, SMEs may lack internal IT expertise, and, consequently, the easiest way for them make a decision about adopting CC is to follow the industry hype or what is suggested by, for example, the media, white papers, and consultants. Table 2 summarizes three types of isomorphic pressure, which result from field-level changes and influence organizations' decisions to adopt or not to adopt CC.

Table 2: Institutional isomorphism

Isomorphism	Description	References
Coercive	Organizations adopt CC for regulatory compliance reasons or because they forced by other organizations through compulsory power.	Chong & Ooi (2008) Zielinski (2009) Low et al. (2011) Herhalt & Cochrane (2012) Li et al. (2012)
Normative	Organizations adopt CC because they are influenced by learning processes or a convincing power of other organizations.	Yao et al. (2010) Low et al. (2011) Herhalt & Cochrane (2012)
Mimetic	Organizations adopt CC to become similar to other adopting organizations, without a thorough reflection process.	Benders et al. (2006) Parakala & Udhas (2011) Sultan (2011)

Strategic responses. Types of isomorphic pressures, to a great extent, influence a set of possible strategic responses that an organization may choose from (see Table 3). An organization that faces a coercive isomorphic pressure from either its parent or regulatory body most likely has no other choice than to adopt CC (Chong & Ooi 2008). Thus, it will adopt an *acquiescence* response. This response may also be a result of a proper study conducted by the potential adopters preceding their decision to adopt full implementation of CC (Herhalt & Cochrane 2012). In another extreme, some organizations choose a *defiance* strategic response by deciding not to adopt CC due to some reason, such as being unsure about the validity of the promises of CC, a lack of customization opportunities, or dissatisfaction with the offerings/pricing by the vendors (Yao et al. 2010; Herhalt & Cochrane 2012). The other possible strategic responses that exist between these two extremes include compromise, avoidance, and manipulation.

Table 3: Strategic responses

Strategy	Example of response	References
Acquiescence	Organizations adopt CC with or without any reflection. Some of them conduct a proper study and decide to choose full implementation, while others do so simply by following the norms, business hype, and/or regulatory force.	Chong & Ooi (2008) Herhalt & Cochrane (2012)
Compromise	Organizations develop an adoption strategy, such as by adopting CC to run parts of their strategic information systems or by combining public and private/community clouds.	Parakala & Udhas (2011) Herhalt & Cochrane (2012)
Avoidance	Organizations adopt partial implementation and conduct testing of a proof of concept, such as using CC to run parts of their nonstrategic information systems.	Herhalt & Cochrane (2012) Lin & Chen (2012)
Defiance	Organizations decide not to adopt CC at all.	Ernst & Young (2012) Herhalt & Cochrane (2012)
Manipulation	Organizations establish their own private or community CC.	Marston et al. (2011) Brian et al. (2012) Herhalt & Cochrane 2012)

For the *compromise* strategic response, organizations may develop an adoption strategy (Herhalt & Cochrane 2012); for example, they may decide to adopt hybrid clouds by keeping mission-critical applications on the private/community cloud and transferring noncritical applications to the public cloud (Parakala & Udhas 2011). Some organizations may use *avoidance* strategic response by adopting partial implementation of CC for purposes of trialability (Herhalt & Cochrane 2012). When an organization decides to adopt a *manipulation* strategic response, they may establish their own private or community cloud (Herhalt & Cochrane 2012). This strategy is most likely to be adopted by LEs or a group of SMEs that want to have full control over their privacy

and service quality. A previous study pointed out that LEs are concerned about the service quality of CC and control over their data; hence, they may implement private CC although it requires capital expenditures (Marston et al. 2011).

To sum up, based on the core concepts of institutional theory and the extant literature, we have contextualized the analytical framework of CC adoption (see Figure 2, an extension of Figure 1). Our framework provides insights to better understand how and why organizations adopt or do not adopt CC to support their business. We have identified a number of relevant organizations that comprise the organizational field: CC providers, peer organizations, business partners, professional and industry associations, and regulators. We have also revealed possible isomorphic pressures that are relevant to studying the adoption of CC. Further, we have attempted to translate five institutional strategic responses proposed by Oliver (1991) into the context of CC adoption.

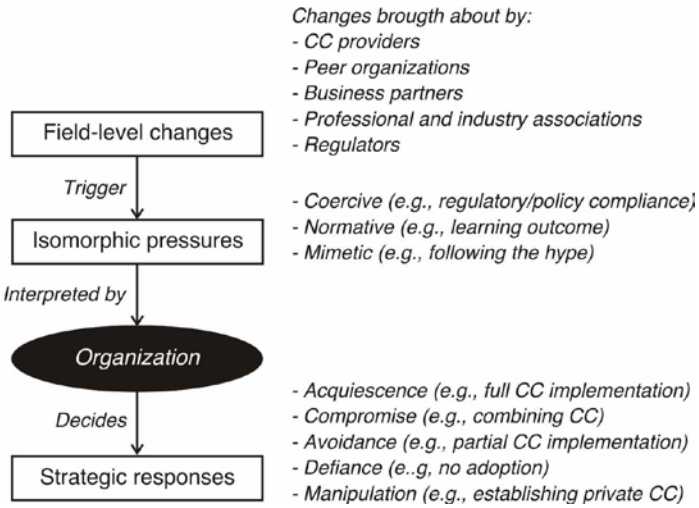


Figure 2: The analytical framework

5. Concluding remarks

We have presented an analytical framework based on core concepts drawn from institutional theory to understand the adoption of CC among organizations. Although it is supported by plausible arguments based on the extant literature, it should not be viewed as a simple checklist and used mechanically. To avoid this trap, future studies may delve further into each concept by tracing the CC adoption process (Suddaby 2010. It is important to note that while some IT innovations have become successfully embedded and routinized in organizations, some are only used at the ceremonial level to gain legitimacy and are decoupled from everyday practices (Meyer & Rowan 1977; DiMaggio & Powell 1983; Boxenbaum & Jonsson 2008; Currie 2009).

This analytical framework does not explicitly pay attention to the *how* and *why* of CC adoption. It is important to understand the process of how an organization interprets the field-level changes, and it is equally important to gain insights into why an organization decides to adopt a certain strategic response over others. Both external and internal factors may be considered in this process. These voids could be addressed through empirical investigation and by bringing in other concepts from either institutional theory, such as institutional work (Lawrence & Suddaby 2006) or institutional logic (Thornton & Ocasio, 2008), or other relevant theories, such as the stakeholder theory (Mitchell et al. 1997). Additionally, this phenomenon can be studied by engaging in interpretive research (Suddaby 2010) and by conducting multiple case study (Mills et al. 2006) with carefully selected organizations from various contexts (such as from developed and developing countries and from different industry sectors). Our hope is that the proposed analytical framework can be validated, fine-tuned, and extended by future research.

References

Altaf, F. and Schuff, D. (2010) "Taking a Flexible Approach to ASPs", *Communication of the ACM*, Vol. 53, No. 2, pp. 139-143.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010) "A View of Cloud Computing", *Communications of The ACM*, Vol. 53, No. 2, pp. 50–58.

Avgerou, C. (2000) "IT and Organizational Change: An Institutionalist Perspective", *Information Technology & People*, Vol. 13, No. 4, pp. 234–262.

Badger, L., Bohn, R., Chu, S., Hogan, M., Liu, F., Kaufmann, V., Mao, J., Messina, J., Mills, K., Sokol, A., Tong, J., Whiteside, F., and Leaf, D. (2011) *US Government Cloud Computing Technology Roadmap Volume I Release 1.0*, National Institute of Standards and Technology, United States.

Benders, J., Batenburg, R. and Van der Blonk, H. (2006) "Sticking to Standards: Technical and Other Isomorphic Pressures in Deploying ERP-systems", *Information & Management*, Vol. 43, No. 2, pp.194–203.

Boxenbaum, E. and Jonsson, S. (2008) "Isomorphism, Diffusion and Decoupling", in Greenwood, R., Oliver, C., Suddaby, R. and Sahlin-Andersson, K. (eds.) *The SAGE Handbook of Organizational Institutionalism,* Sage, London, pp. 78–98.

Brian, H. A. Y. E. S., Brunschwiler, T., Dill, H., Christ, H., Falsafi, B., Fischer, M. et al. (2008) "Cloud Computing", *Communications of the ACM*, Vol. 51, No. 7, pp. 9–11.

Catteddu, D. (2010) "Cloud Computing: Benefits, Risks and Recommendations for Information Security", in Serrão, C., Díaz, V.A. and Cerullo, F. (eds.) *Web Application Security*, Springer, Berlin Heidelberg.

Chong, A.Y.-L. & Ooi, K.-B. (2008) "Adoption of Interorganizational System Standards in Supply Chains: An Empirical Analysis of RosettaNet standards", *Industrial Management & Data Systems*, Vol. 108, No. 4, pp. 529–547.

Covaleski, M.A. & Dirsmith, M.W. (1988) "An Institutional Perspective on the Rise, Social Transformation, and Fall of a University Budget Category", *Administrative Science Quarterly*, Vol. 33, No. 4, pp. 562–587.

CSA & ISACA (2012) *Cloud Computing Market Maturity*, CSA & ISACA.

Currie, W. (2009) "Contextualising the IT Artefact: Towards a Wider Research Agenda for IS Using Institutional Theory", *Information Technology & People*, Vol. 22, No.1, pp. 63–77.

Dillon, T., Wu, C. and Chang, E. (2010) "Cloud Computing: Issues and Challenges", *Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),* pp. 27–33.

DiMaggio, P. and Powell, W. (1983) "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review*, Vol. 48, No. 2, pp. 147–160.

Dowling, J. and Pfeffer, J. (1975) "Organizational Legitimacy: Social Values and Organizational Behavior", *The Pacific Sociological Review*, Vol. 18, No. 1, pp. 122–136.

Durkee, D. (2010) "Why Cloud Computing Will Never be Free", *Communications of the ACM*, Vol. 53, No. 5, p. 62.

Ernst & Young (2011) *Cloud Computing Issues and Impacts*, Ernst & Young, United Kingdom.

Ernst & Young, 2012. *Ready for Takeoff: Preparing for Your Journey Into the Cloud*, Ernst & Young, United Kingdom.

Garrison, G., Kim, S. and Wakefield, R.L. (2012) "Success Factors for Deploying Cloud Computing", *Communications of the ACM*, Vol. 55, No. 9, pp. 62–68.

Gordon, J., Hayashi, C., Elron, D., Huang, L. and Neill, R. (2010) *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-driven Transformation,* World Economic Forum, Geneva.

Heart, T. (2010) "Who is Out There ? Exploring the Effects of Trust and Perceived Risk on SaaS Adoption Intentions", *The DATA BASE for Advances in Information Systems*, Vol. 41, No. 3, pp. 49–68.

Herhalt, J. and Cochrane, K. (2012) *Exploring the Cloud: A Global Study of Governments' Adoption of Cloud*, KPMG.

Kepes, B. (2011) *Cloudonomics: The Economics of Cloud Computing*, Diversity Limited, United States.

Kshetri, N. (2012) "Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution", *Telecommunications Policy*, Vol. 37, Nos. 4/5, pp. 372–386

Lawrence, T.B. and Suddaby, R. (2006) "Institutions and Institutional Work", in Clegg, S., Hardy, C., Lawrence, T.B., and Nord, W.R. (eds.) *The SAGE Handbook of Organization Studies,* Sage, London, pp. 215–254.

Lee, C., Mckean, J. and King, J. (2011) *CIO Global Cloud Computing Adoption Survey Results*, CIO/IDG Research Services.

Li, M., Yu, Y., Zhao, L. J., Li, X. (2012) "Drivers for Strategic Choice of Cloud Computing as Online Services in SMEs", *Proceedings of the International Conference on Information Systems (ICIS)*.

Lin, A. and Chen, N. (2012) "Cloud Computing as an Innovation: Perception, Attitude, and Adoption", *International Journal of Information Management*, Vol. 32, No. 6, pp. 533–540.

Low, C., Chen, Y. and Wu, M. (2011) "Understanding the Determinants of Cloud Computing Adoption", *Industrial Management & Data Systems*, Vol. 111, No. 7, pp. 1006–1023.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011) "Cloud Computing: The Business Perspective", *Decision Support Systems*, Vol. 51, No. 1, pp. 176–189.

Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, United States.

Meyer, J.W. and Rowan, B. (1977) "Institutionalized Organizations : Formal Structure as Myth and Ceremony", *American Journal of Sociology*, Vol. 83, No. 2, pp. 340–363.

Mignerat, M. and Rivard, S. (2009) "Positioning the Institutional Perspective in Information Systems Research", *Journal of Information Technology*, Vol. 24, No. 4, pp. 369–391.

Mills, M., Van De Bunt, G.G. and De Bruijn, J. (2006) "Comparative Research: Persistent Problems and Promising Solutions", *International Sociology*, Vol. 21, No. 5, pp. 619–631.

Mitchell, R.K., Agle, B.R. and Wood, D.J. (1997) "Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts", *Academy of Management Review*, Vol. 22, No. 4, pp. 853–886.

Mouritsen, J. (1994) "Rationality, Institutions And Decision Making: Reflections on March and Olsen's Rediscovering Institutions", *Accounting Organizations and Society*, Vol. 19, No. 2, pp. 193–211.

Oliver, C. (1991) “Strategic Responses to Institutional Processes”, *Academy of Management Review*, Vol. 16, No. 1, pp. 145–179.

Orlikowski, W.J. and Barley, S.R. (2001) "Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn From Each Other?", *MIS Quarterly*, Vol. 25, No. 2, pp. 145–165.

Parakala, K. and Udhas, P. (2011) *The Cloud: Changing the Business Ecosystem*, KPMG.

Scott, W.R. (2004) “Institutional Theory: Contributing to a Theoretical Research Program”, in Smith, K.G. and Hitt, M.A. (eds.) *Great Minds in Management: The Process of Theory Development,* pp. 460–484, Oxford University Press, Oxford, UK.

Scott, W.R. (2001) *Institutions and Organizations*, Sage, London.

Scott, W.R. (1991) “Unpacking Institutional Arguments”, in Powell, W.W. and DiMaggio, P.J. (eds.) *The New Institutionalism in Organizational Analysis*, University of Chicago Press, Chicago, pp. 143–163.

Son, I., Lee, D., Lee, J. N. and Chang, Y.B. (2011). “Understanding the Impact of IT Service Innovation on Firm Performance: The Case of Cloud Computing”, *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*.

Suchman, M.C. (1995) “Managing Legitimacy: Strategic and Institutional Approaches”, *Academy of Management Review*, Vol. 20, No. 3, pp. 571–610.

Suddaby, R. (2010) “Challenges for Institutional Theory”, *Journal of Management Inquiry*, Vol. 19, No. 1, pp. 14–20.

Sultan, N.A. (2011) “Reaching for the “cloud”: How SMEs Can Manage”, *International Journal of Information Management*, Vol. 31, No. 3, pp. 272–278.

Swanson, E.B. and Ramiller, N.C. (2004) “Innovating Mindfully with Information Technology”, *MIS Quarterly*, Vol. 28, No. 4, pp. 553–583.

Thornton, P.H. and Ocasio, W. (2008), "Institutional Logics", in Greenwood, R., Oliver, C., Suddaby, R. and Sahlin-Andersson, K. (eds.) *The SAGE Handbook of Organizational Institutionalism*, Sage, London, pp. 99-129.

Timmermans, J., Ikonen, V., Stahl, B.C. and Bozdag, E. (2010) “The Ethics of Cloud Computing: A Conceptual Review”, *Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science*, pp. 614–620.

Tolbert, P.S. and Zucker, L.G. (1996) “The Institutionalization of Institutional Theory”, in Clegg, S.R., Hardy, C. and Nord, W.R. (eds.) *Handbook of Organization Studies*, Sage, London, pp. 175–190.

Venters, W. and Whitley, E.A. (2012) “A Critical Review of Cloud Computing: Researching Desires and Realities”, *Journal of Information Technology*, Vol. 27, No. 3, pp. 179–197.

Weerakkody, V., Dwivedi, Y.K. and Irani, Z. (2009) “The Diffusion and Use of Institutional Theory: A Cross-Disciplinary Longitudinal Literature Survey”, *Journal of Information Technology*, Vol. 24, No. 4, pp. 354–368.

Weinhardt, C., Anandasivam, D.I.W.A., Blau, B., Borissov, D.I.N., Meinl, D.M.T., Michalk, D.I.W.W. and Stößer, J. (2009) “Cloud Computing: A Classification, Business Models, and Research Directions”, *Business Information Systems Engineering*, Vol. 1. No. 5, pp. 391–399.

Wooten, M. and Hoffman, A.J. (2008) “Organizational Fields: Past, Present and Future”, in Greenwood, R., Oliver, C., Suddaby, R. and Sahlin-Andersson, K. (eds.) *The SAGE Handbook of Organizational Institutionalism,* Sage, London, pp. 130–147.

Yang, H. and Tate, M. (2012) “A Descriptive Literature Review and Classification of Cloud Computing Research”, *Communications of the Association for Information Systems*, Vol. 31, No. 1, pp. 35-60.

Yao, Y., Watson, E. and Khan, B. K. (2010) “Application Service Providers: Market and Adoption Decisions”, *Communications of the ACM*, Vol. 53, No. 7, pp. 113–117.

Zielinski, D. (2009) “Be Clear on Cloud Computing Contracts”, *HR Magazine*, Vol. 54, No. 11, pp. 63–65.

A Literature Review on Cloud Computing Adoption Issues in Enterprises

Rania Fahim El-Gazzar

Department of Information Systems, University of Agder, Kristiansand, Norway
rania.f.el-gazzar@uia.no

Abstract. Cloud computing has received increasing interest from enterprises since its inception. With its innovative information technology (IT) services delivery model, cloud computing could add technical and strategic business value to enterprises. However, cloud computing poses highly concerning internal (e.g., Top management and experience) and external issues (e.g., regulations and standards). This paper presents a systematic literature review to explore the current key issues related to cloud computing adoption. This is achieved by reviewing 51 articles published about cloud computing adoption. Using the grounded theory approach, articles are classified into eight main categories: internal, external, evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation. Then, the eight categories are divided into two abstract categories: cloud computing adoption factors and processes, where the former affects the latter. The results of this review indicate that enterprises face serious issues before they decide to adopt cloud computing. Based on the findings, the paper provides a future information systems (IS) research agenda to explore the previously under-investigated areas regarding cloud computing adoption factors and processes. This paper calls for further theoretical, methodological, and empirical contributions to the research area of cloud computing adoption by enterprises.

Keywords: Cloud computing, adoption, enterprise.

1 Introduction

Over the past decade, there has been a heightened interest in the adoption of cloud computing by enterprises. Cloud computing promises the potential to reshape the way enterprises acquire and manage their needs for computing resources efficiently and cost-effectively [1]. In line with the notion of shared services, cloud computing is considered an innovative model for IT service sourcing that generates value for the adopting enterprises [2]. Cloud computing enables enterprises to focus on their core business activities, and, thus, productivity is increased [3]. The adoption of cloud computing is growing rapidly due to the scalability, flexibility, agility, and simplicity it offers to enterprises [3–6]. A recent cross-sectional survey by [7] on the adoption rates of cloud computing by enterprises reported that 77% of large enterprises are adopting the cloud, whereas 73% of small and medium-sized enterprises (SMEs) are adopting the cloud.

B. Bergvall-Kåreborn and P.A. Nielsen (Eds.): TDIT 2014, IFIP AICT 429, pp. 214–242, 2014.

Cloud computing is "an old idea whose time has (finally) come" [8]. The term cloud is old since it was drawn in network diagrams as a metaphor representing the Internet [9]. Cloud computing is generally referred to as providing "Internet-based computing service" [10]; however, the technical meaning is richer, as cloud computing builds on already-existing computing technologies, such as grid computing and virtualization, which are forms of distributed computing technology [9]. Virtualization involves masking the physical characteristics of computing resources to hide the complexity when systems, applications, or end users interact with them [9]. Grid computing is "a model of distributed computing that uses geographically and administratively distant resources, and, thus, users can access computers and data transparently without concern about location, operating system, and account administration" [11]. With the advent of cloud computing, the merits of virtualization and grid computing have been combined and further improved. Cloud computing shares some characteristics with virtualization and grid computing; however, it still has its own distinguishing characteristics as well as associated risks [12–15].

Cloud computing has been given numerous definitions since its advent. Basically, definitions started with the notion of an application service provision (ASP) that is an IT sourcing model for renting business applications over the Internet [16]. This definition became wider as Internet-based IT service offerings comprised storage, hosting infrastructure, and network; thus, it is given the name net sourcing, to fit the variety of IT service offerings [17]. HP defines cloud computing as "Everything as a Service" [18], while Microsoft perceives the value of cloud computing as "Cloud + Client," emphasizing the importance of the end user [19]. T-Systems define cloud computing as "the renting of infrastructure and software, as well as bandwidths, under defined service conditions. These components should be able to be adjusted daily to the needs of the customer and offered with the utmost availability and security. Included in cloud computing are end-2-end service level agreements (SLAs) and use-dependent service invoices" [20].

T-Systems' definition conveys the idea of cloud computing as being a utility computing or 5th utility, because enterprises are able to consume computing resources on a pay-as-you-go basis just like the four public utilities (water, electricity, gas, and telephone). The widely known definition of cloud computing is by the National Institute of Standards and Technology (NIST). The NIST defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [21]. According to the NIST definition, the basic actors in the cloud computing context are the cloud service provider (CSP) and the cloud service consumer (CSC), despite that there might be service brokers involved [22].

CSPs offer various service models depending on the enterprise's requirements, whereas the basic service models are [21]: (1) Software-as-a-Service (SaaS), the capability of the consumer to use the provider's applications running on a cloud infrastructure; (2) Platform-as-a-Service (PaaS), the capability of the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider; and (3) Infrastructure-as-a-Service (IaaS), the capability of the consumer to provision

processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. It has been reported that 32% of large enterprises are testing the concept of cloud computing; 37% are already running applications on the cloud; and 17% are using cloud infrastructure [7]. Contrarily, 19% of SMEs are testing the concept; 29% are running applications on the cloud; and 41% are using cloud infrastructure [7].

Cloud computing service models share five common essential characteristics that distinguish cloud computing from other computing technologies [21]:

1. On-demand self-service, where the consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider;
2. Broad network access, where the capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations);
3. Resource pooling, where the provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand;
4. Rapid elasticity, where capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand; and
5. Measured service, where cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

Cloud service models can be deployed in one of the four deployment models [21]: (1) private cloud, where the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units), and it may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises; (2) community cloud, where the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations), and it may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises; (3) public cloud, where the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them, and it exists on the premises of the cloud provider; (4) hybrid cloud, where the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). It has been reported recently that 61% of enterprises are currently using public clouds; 38% are using private clouds; and 29% are using hybrid clouds [7].

At the enterprise level, cloud computing adoption takes place in three contexts. Large enterprises have slack resources, both financial and technical, to afford deploying private IaaS, PaaS, and SaaS clouds on a pay-as-you-go basis [4, 23]. Whereas, SMEs tend to deploy public SaaS clouds, which are appropriate for their start-up due to their limited financial and IT capabilities, which impede their deploying and maintaining private clouds [4, 24–26]. For governments, deployment of private IaaS clouds is favorable [4].

In spite of its appealing benefits for enterprises, cloud computing raises serious technical, economic, ethical, legal, and managerial issues [6, 27]. The extant literature is focused more on the technical issues of cloud computing, with less attention paid to business issues regarding the adoption of cloud computing [10]. Further, there is a lack of in-depth studies about issues related to the cloud computing adoption process in the context of enterprise users [10, 28]. The purpose of this study is to review systematically the extant literature regarding cloud computing adoption to identify the key issues that have been researched. In addition, the quality of the extant research will be assessed. Then, the under-researched areas will be identified, and a future IS research agenda will be proposed accordingly. The remainder of this study is organized as follows: Section 2 presents the methodology of the systematic literature search process and the classification schemes adopted. Section 3 presents the findings from the review. Implications for future IS research are discussed in Section 4. Conclusions of this review are presented in Section 5.

2 Research Method

Reviewing the literature is an essential process that creates a firm foundation for advancing knowledge; it facilitates uncovering areas where research is needed [29]. This paper aims at systematically reviewing the literature to represent the current state of IS research regarding cloud computing adoption issues. This review process followed the fundamental guidelines for conducting an effective literature review by [29–31], and it is done within boundaries [29]. The contextual boundary for this review is the enterprise users, not individuals, as there are significant issues that need to be addressed before enterprises start using clouds [27, 32]. The temporal boundary of this review covers the published articles in all previous years until February 2014.

2.1 Literature Search Process

The literature search process of this review involved querying seven quality scholarly literature databases (AISeL, IEEE Xplore, ScienceDirect, EBSCOhost, ProQuest, Wiley online library, and ACM digital library). These databases provide access to leading IS journals and high-quality peer-reviewed IS conference publications [31]. Further, online databases are appropriate and practical sources for reviewing the literature about a contemporary phenomenon such as cloud computing [10]. The search criterion was limited to the article's title to ensure the relevance of the articles. The terms used for searching all seven databases are 'cloud computing' in combination with 'adopt*' and other related terms, such as 'accept*' and 'diffus*'. This initially resulted in 94 articles in total including recurrences. An overview of the search process is provided in Table 1.

Table 1. Literature search overview

Literature databases	Search query	Search results
AISeL	title:"cloud computing" AND title:adopt*	15
	title:"cloud computing" AND title:accept*	2
	title:"cloud computing" AND title:diffus*	0
IEEE Xplore	(("Document Title":"cloud computing") AND "Document Title":"adopt*")	22
	(("Document Title":"cloud computing") AND "Document Title":"accept*")	2
	(("Document Title":"cloud computing") AND "Document Title":"diffus*")	1
ScienceDirect	TITLE("cloud computing") and TITLE(adopt*)	6
	TITLE("cloud computing") and TITLE(accept*)	0
	TITLE("cloud computing") and TITLE(diffus*)	0
EBSCOhost	TI "cloud computing" AND TI "adopt*"	30
	TI "cloud computing" AND TI "accept*"	0
	TI "cloud computing" AND TI "diffus*"	1
ProQuest	ti("cloud computing") AND ti(adopt*)	6
	ti("cloud computing") AND ti(accept*)	1
	ti("cloud computing") AND ti(diffus*)	0
Wiley (Online Library)	"cloud computing" in Article Titles AND "adopt*" in Article Titles	1
	"cloud computing" in Article Titles AND accept* in Article Titles	1
	"cloud computing" in Article Titles AND diffus* in Article Titles	0
ACM (Digital Library)	(Title:"cloud computing" and Title:"adopt*")	5
	(Title:"cloud computing" and Title:"accept*")	1
	(Title:"cloud computing" and Title:"diffus*")	0
Total		94

The practical screen involved reading the abstract of the articles to decide their relevance to the focus of this review [30, 33]. Further, the filtering criteria involved the exclusion of recurring articles, research-in-progress articles, articles that were not written in English, articles with a focus on individuals, periodical articles published by news websites, trade journals, and magazines. These exclusion criteria delimit the sample of articles so that the literature review becomes practically manageable [33]. Eventually, this resulted in 51 articles for the classification.

2.2 Classification Scheme

The reviewed articles are classified according to the research methods employed in each study to identify how adequately the adoption of cloud computing is researched [34–36]. The research methods used in the reviewed articles are lab experiments, field studies, Delphi study, interviews, literature reviews, case studies, and surveys. Some articles do not have a methodology section and reflect on some concepts in relation to cloud computing (i.e., cost, security, performance, etc.) or they adopt theories without empirical testing. This group of articles is labeled as “conceptual papers.”

Cloud computing adoption issues are discussed diversely in the literature; thus, this review sought to develop a classification scheme to better gain insights from the

preceding academic contributions to the area of cloud computing adoption. The classification of the 51 articles involved using a bottom-up grounded theory (GT) approach [37]. The GT approach is said to be valuable for conducting a rigorous literature review [38], "instead of force-fitting the data to an a priori theory" [39]. The 51 reviewed articles are classified according to a GT approach for reviewing the literature recommended by [38]. Using a GT approach in reviewing the literature helps "reach a thorough and theoretically relevant analysis of a topic" [38].

The classification process involved a close reading of the articles. Then, the open coding was utilized to generate codes from analyzing each article's text to capture the themes that appear in each article. This resulted in 30 concepts, which were labeled. Next, the axial coding was applied to develop the relations between the concepts identified in the open coding [38]. This resulted in a grouping of the 30 subcategories identified from the open coding into eight corresponding categories (i.e., internal, external, evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation).

Finally, the selective coding technique was applied to integrate and refine the eight main categories and to develop relations between them [38]. This resulted in two abstract categories: cloud adoption factors (i.e., internal and external) and cloud adoption processes (i.e., evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation), where the former influenced the latter (see Table 2).

Table 2. Classification scheme

Selective coding	Axial coding	Open coding
1. Cloud computing adoption factors	1. External	1. Government regulations
		2. IT industry standards institutes
		3. Cloud providers
		4. Business partners
		5. Competitors
		6. Cloud service broker
	2. Internal	7. Willingness to invest
		8. Top management
		9. Firm size
		10. Organizational culture
		11. Employees' IT skills
		12. Prior experience
2. Cloud computing adoption processes	3. Evaluation	13. Cost and benefits
		14. Impact on people and work practices
		15. Internal readiness
		16. Cloud provider selection
	4. Proof of concept	17. Trialability
		18. Perceived benefits and risks
	5. Adoption decision	19. Business needs identification
		20. Criticality determination
		21. Strategic value evaluation
		22. Implementation planning
		23. Service model selection
		24. Deployment model selection
		25. Contract and SLA negotiation

Table 2. (*Continued*)

6.	Implementation and integration	26. Complexity 27. Compatibility
7.	IT governance	28. Auditability and traceability 29. Risk management
8.	Confirmation	30. Usage continuance

3 Findings

The findings from reviewing 51 articles are presented in light of six dimensions: distribution of articles over years, outlets in which articles were published, theories/frameworks used, research methods used, and cloud computing adoption factors and processes. Fig. 1 illustrates that interest in researching the topic of cloud computing adoption has grown exponentially from 2009 until 2013, denoting that cloud computing adoption is remarkable. However, the three articles published in 2014 do not present a full picture of research endeavors of the whole year 2014.

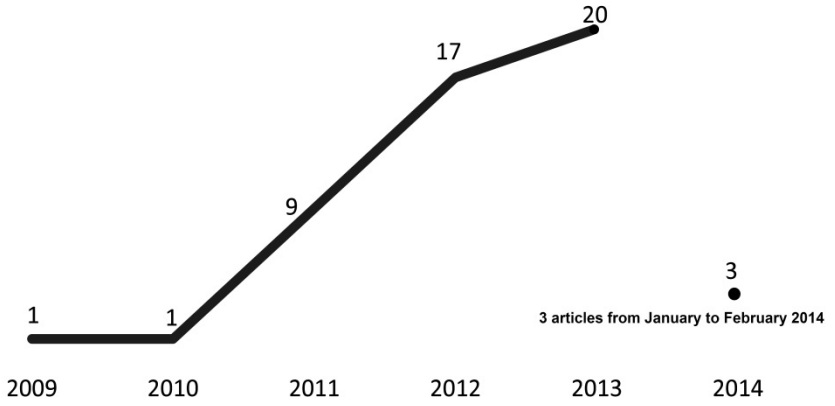


Fig. 1. Distribution of articles over years

The outlets in which the articles were published and the number of articles (N) in each are presented in Table 3; the outlets are categorized as IS and non-IS journals and conferences. The IS journals and conferences are identified according to the Association for Information Systems (AIS)[1,2,3,4] and [31]. Obviously, non-IS journals dominate in investigating cloud computing adoption area with 11 articles each, whereas only one IS journal contributed with three articles. Likewise, non-IS conferences contributed numerously, with 25 articles, whereas IS conferences had 12 articles. However, more published articles were found in IS conference publications than in IS journals.

[1] http://aisnet.org/general/custom.asp?page=JournalRankings
[2] http://aisnet.org/?AffiliatedConference
[3] http://aisnet.org/?page=Conferences
[4] http://aisel.aisnet.org/affiliated/

Table 3. Number of articles per outlet type

Outlet type	Outlet name	N
IS Journals	• International Journal of Information Management	3
Non-IS Journals	• Journal of Technology Management for Growing Economies • Journal of Medical Marketing: Device, Diagnostic and Pharmaceutical Marketing • Mathematical and Computer Modelling • Industrial Management & Data Systems • International Journal of Logistics Management • Journal of Enterprise Information Management • IEEE Transactions on Engineering Management • European Management Review • Procedia Technology • Journal of Industry, Competition, and Trade • GSTF Journal on Computing	11
IS Conferences	• International Conference on Information Systems (ICIS) • Americas Conference on Information Systems (AMCIS) • Hawaii International Conference on System Sciences (HICSS) • European Conference on Information Systems (ECIS) • Pacific Asia Conference on Information Systems (PACIS) • Mediterranean Conference on Information Systems (MCIS)	12
Non-IS Conferences	• International Conference for Internet Technology and Secured Transactions (ICITST) • BLED Conference • International Conference on Networked Computing and Advanced Information Management (NCM) • International Conference on Cloud Computing Technology and Science • International Conference on System of Systems Engineering • International Conference on Adaptive Science & Technology (ICAST) • European Conference on Information Management & Evaluation • International Conference on Product Focused Software Development and Process Improvement • International Conference on Information Integration and Web-based Applications & Services (iiWAS) • Annual Allerton Conference on Communication, Control, and Computing (Allerton) • International Conference on Cloud Computing (CLOUD) • International Conference on Advances in Computing, Communications, and Informatics • International Conference on Computing, Management and Telecommunications (ComManTel) • International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM) • International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM) • UK Academy for Information Systems Conference • International Conference on Computer and Information Science	25

Table 3. (*Continued*)

• IST-Africa Conference and Exhibition • International Conference on Research and Innovation in Information Systems (ICRIIS) • International Conference on ICT for Smart Society • IEEE World Congress on Services

The findings from the 51 articles are further organized according to theory/framework/model used in each publication. Some articles discuss related concepts (i.e., performance, cost, security, cloud providers, etc.); thus, they are considered to be using "general concepts." Further, other articles use a GT approach to understand cloud computing adoption; these articles built models based on field data. The use of different theories to understand cloud computing adoption factors and processes is quite evident, as per Table 4. Further, articles that tested theories empirically by field data are predominant, but the non-empirically tested theoretical contributions are not slight. General concepts are the most frequently used to explain cloud computing adoption factors and processes.

The use of the technology-organization-environment (TOE) framework is also frequent compared to other theories, followed by diffusion of innovation (DOI) theory and the GT approach, which appear to be the next most frequently used in the reviewed articles. Empirically tested theories/frameworks/models are dominant with 34 articles, whereas studies with no empirical testing were less common: 17 articles. However, the number of articles without empirical testing is still remarkable, which implies the need for more field work. Further, the majority of articles used a combination of multiple theoretical perspectives to gain more insights about cloud computing adoption factors and processes. This implies that cloud computing adoption phenomenon is multifaceted. The majority of articles have used theories/frameworks/models to explain what are the factors that affect the adoption of cloud computing and what are the key considerations in cloud computing adoption processes. Yet, there is a lack of using theories that demonstrate how enterprises react differently to same internal and external factors and why do they react in such a way.

Table 4. Use of theory by reviewed articles

Theory (T)/Framework(F)/Model(M)		References (Empirical Testing)	References (no Empirical Testing)	Frequency
(M)	Technology Acceptance Model (TAM)	[40], [41], [42]	-	3
(M)	Post-Acceptance Model (PAM) of IS Continuance	[43]	-	1
(T)	Utility Theory	[44]	-	1
(M)	Human-Organization-Technology Fit Model (HOT-fit)	[45]	-	1
(M)	Business Model Factors	[46]	-	1
(M)	Structural Equation Modeling (SEM)	[47]	-	1

Table 4. (*Continued*)

(F)	Technology-Organization-Environment (TOE)	[48], [49], [50], [51], [52], [45], [53], [54], [55]	[56], [23]	11
(T)	Organizational Information Processing Theory	[57]	-	1
-	General Concepts	[58], [59], [60], [61], [62], [63]	[64], [65], [66], [67], [68], [69], [70], [71], [72]	15
(F)	National Outsourcing Association (NOA) Framework for Factors Inhibiting Cloud Computing Adoption	[73]	-	1
(F)	Contextual Usability Framework	[74]	-	1
(F)	Attention Based View (ABV)	[75]	-	1
(T)	Diffusion Of Innovation (DOI)	[76], [40], [74]	[56], [23], [77]	6
(T)	Transaction Cost Economics (TCE) Theory	-	[78], [77]	2
(T)	Resource Dependence Theory (RDT)	-	[77]	1
(T)	Innovation Decision Process Theory (IDPT)	-	[79]	1
(T)	Dynamic Capabilities Theory	[40]	-	1
(T)	Contingency Theory	[40]	-	1
(T)	Mean Field Game Theory (MFG)	-	[80]	1
(M)	Return On Investment (ROI)	-	[81]	1
(T)	Option Pricing Theory	-	[82]	1
(T)	Perceived Attributes Theory	-	[79]	1
(F)	Geoffrey Moore's Technology Adoption Life Cycle	-	[79]	1
(F)	Innovation Value Institute's IT Capability Maturity Framework (ITCMF)	[83]	-	1
(T)	Actor Network Theory (ANT)	[48], [55]	-	2
(M)	Gap Analysis Model	[84]	-	1
(T)	GT Approach	[85], [86], [87], [88], [89]	-	5
Total (without repetitions)		34	17	

As per Table 5, the 51 articles are mapped to cloud computing adoption factors (i.e., external and internal) and processes (i.e., evaluation, proof of concept, adoption decision, implementation and integration, IT governance, and confirmation) identified in this review as well as research methods (RM) employed (i.e., Lab Experiment (LE), Field Study (FS), Case Study (CS), Delphi Study (DS), Survey (SUR), Interviews (INT), Conceptual Paper (CP), Literature Review (LR)). Further, the number of articles (N) per subcategory and research method is provided. The findings, in general,

indicate fewer qualitative studies (i.e., case studies, interviews, and field studies) have contributed to the understanding of cloud computing adoption factors and processes, as compared to quantitative studies (i.e., surveys). In some articles, multiple methods are used [42, 44, 50, 57]. Further, external adoption factors are extensively addressed by survey and conceptual articles, and less addressed by in-depth studies. This applies similarly to the internal factors. Among the external factors, investigating government regulations is dominant. Regarding the internal factors, the role of top management in cloud computing adoption is more researched among others. In general, adoption processes, such as evaluation, adoption decision, implementation and integration, IT governance, and confirmation, are not adequately addressed, except for the proof of concept process. However, the number of studies identifying perceived benefits and risks is predominant in proof of concept process and among other cloud computing adoption processes.

Table 5. Mapping of articles to classification scheme and research methods

Cloud computing adoption factors and processes		LE	FS	CS	DS	SUR	INT	CP	LR
External factors	Government regulations (N = 20)	-	[61]	[83], [48], [89], [84]	[57], [87]	[57], [73], [54], [50], [55], [45]	[57], [50]	[23], [77], [69], [78], [68], [79], [72], [70]	-
	IT industry standards institutes (N = 6)	-	-	[83]	-	[76], [54]	-	[77], [78], [71]	-
	Cloud providers (N = 15)	-	-	[51], [48], [89]	-	[75], [86], [76], [85], [55], [53], [46]	-	[78], [79], [68], [77], [72]	-
	Business partners (N = 11)	-	-	[48]	[57]	[52], [76], [57], [75], [85], [85], [55], [74], [42], [53]	[57], [42]	[56]	-
	Competitors (N = 10)	-	-	[51], [48]	[57]	[57], [52], [50], [55], [53], [45]	[57], [50]	[23], [56]	-

Table 5. (*Continued*)

	Cloud service broker (N = 1)	-	-	-	-	-	-	[71]	-
Internal factors	Willingness to invest (N = 11)	-	-	[83], [40], [48], [51]	-	[60], [76], [50], [44], [41]	[50], [44]	[23], [56]	-
	Top management (N = 18)	-	[88]	[40], [51], [83], [49]	[87]	[50], [73], [60], [55], [74], [53], [45]	[50]	[67], [23], [81], [64]	-
	Firm size (N = 9)	-	-	-	-	[52], [50], [60], [55], [53]	[50]	[23], [56], [81], [72]	-
	Organizational culture (N = 5)	-	-	[49], [83]	-	[50], [47]	[50]	[71]	-
	Employees' IT skills (N = 8)	-	-	[49]	-	[60], [50], [52], [55], [45]	[50]	[23], [70]	-
	Prior experience (N = 6)	-	-	[51]	-	[41], [74], [42], [53]	[42]	-	-
Evaluation process	Cost and benefits (N = 10)	-	[61]	[89], [84]		[45], [46]	-	[81], [80], [79], [82], [70]	-
	Impact on people and work practices (N = 7)	-	[61]	[83], [89]	-	[42], [41]	[42]	[70], [71]	-
	Internal readiness (N = 7)	-	[88]	[84]	-	[76], [52], [42], [45]	[42]	[23]	-
	Cloud provider selection (N = 6)	-	[61]	[40], [83], [84]	-	-	-	[65], [67]	-
Proof of concept process	Trialability (N = 4)	-	-	[51]	-	[76], [74], [53]	-	-	-

Table 5. (*Continued*)

	Perceived benefits and risks (N = 30)	[62]	-	[51], [40], [49], [48], [89], [84]	-	[50], [86], [63], [75], [54], [76], [85], [73], [59], [41], [55], [74], [42], [53], [45], [46]	[50], [42]	[56], [64], [65], [77], [68], [70], [71]	-
Adoption decision process	Business needs identification (N = 4)	-	[61]	-	-	[76], [53]	-	[64]	-
	Criticality determination (N = 3)	-	-	-	-	-	-	[69], [81], [82]	-
	Strategic value evaluation (N = 3)	-	-	[89]	-	[75], [76]	-	-	-
	Implementation planning (N = 2)	-	-	-	-	[60]	-	[79]	-
	Service model selection (N = 2)	-	-	-	-	-	-	[65]	[66]
	Deployment model selection (N = 2)	-	-	-	-	-	-	[79], [69]	-
	Contract and SLA negotiation (N = 4)	-	-	-	-	[53]	-	[65], [81], [71]	-
Implementation and integration process	Complexity (N = 10)	-	-	[49], [51]	-	[50], [76], [52], [74], [42], [53], [45]	[50], [42]	[23]	-
	Compatibility (N = 9)	-	-	[51]	-	[50], [76], [52], [74], [53], [45]	[50]	[23], [70]	-

Table 5. (*Continued*)

IT governance process	Auditability and traceability (N = 6)	-	-	[49], [83]	-	[50]	[50]	[65], [81], [71]	-
	Risk management (N = 5)	[62]	-	-	-	[63]	-	[69], [71]	[66]
Confirmation process	Usage continuance (N = 2)	-	-	-	-	[43]	-	[79]	-
N per RM		1	2	6	2	24	4	17	1

Cloud Computing Adoption Factors. These comprise internal and external factors that have impact on the cloud computing adoption processes.

External Factors. These comprise factors from the outside social environment in which the enterprise operates and by which its cloud computing adoption process is influenced. These external factors are: 1) government regulations, 2) IT industry standards institutes, 3) cloud providers, 4) business partners, 5) competitors, and 6) cloud service broker. The adoption of cloud computing is arguably surrounded by different levels of environmental and inter-organizational uncertainties [57]. There is a wide emphasis on the importance of *government regulations* at the national and international levels [23, 54, 73, 77]. In spite of their role in facilitating the cloud computing adoption securely, the lack of government regulations can hinder enterprises from adopting the cloud [45, 54, 87]. Some regulations, such as the Sarbanes-Oxley Act (SOX) for corporate accounting data, the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA) were enacted before cloud computing was becoming increasingly adopted, and they might not be sufficient to facilitate its adoption [69, 72]. However, some countries started to enact laws specific to cloud computing, such as *cloud first policy* and the Health Information Technology for Economic and Clinical Health (HITECH) Act in the USA and *cloud computing strategy* by the Australian government [72, 78].

The inconsistency of international government regulations is a further concern as there is no widely agreed data privacy policy among all governments [72]. Some countries tend to restrict enterprises to store their data in cloud infrastructure only if it is within the national borders [68]. For instance, the EU's privacy laws prohibit the exchange of personal information outside the users' jurisdiction [83]. This is because cloud providers running outside of their home country must comply with the host country's regulations and government surveillance, which can be difficult for enterprises to cope with [61, 78]. An example of the multijurisdictional politics that have negative impact on cloud computing adoption is the USA Patriot Act, which makes countries, especially, the EU countries, skeptical about dealing with US-based cloud providers [70, 72]. However, some cloud providers solved this issue to accord with EU data regulations by allowing enterprises to deploy their IT resources on physical servers located within the EU region [70]. Although government regulations are in place in the developed world, they often conflict with each other, and they are not adequately placed in the developing world [72, 78].

In line with this, *IT standards institutes* are also cited as an important factor for dealing with enterprises' concerns about security and the interoperability of cloud solutions [77, 83]. Although they are still missing pieces in the puzzle of cloud computing for enterprises [54, 76, 78], some efforts to develop security standards have occurred; for instance, Cloud Security Alliance (CSA)'s document Security Guidance for Critical Areas of Focus in Cloud Computing for managing cloud computing risks [83]. *Cloud providers* would have to comply with government regulations and industrial standards to gain liability, reputation, and trustworthiness among their potential and present enterprise users [78]. Additionally, they are required to be transparent in explaining information to enterprises about possible benefits and risks from adopting cloud computing [79]. Cloud providers build their reputations by their experience in managing enterprises' needs and concerns in a responsible manner [68, 75, 77]. This is enabled by delivering the promised benefits from cloud computing to enterprises (i.e., service quality, service availability, and service recovery) and protecting their data from potential threats; for instance, in case the cloud provider went out of business [46, 77, 86]. Further, cloud providers' demonstration of successful business cases and models are likely to increase cloud computing adoption rates [51, 76]. Moreover, the support for implementing and using cloud services made available by cloud services providers is likely to motivate enterprises to adopt cloud computing [53]. however, cloud providers might trigger a major concern for enterprises if they outsource some of their services to another service provider [77]. In this regard, trust issues are not well-explored yet.

Observing that *business partners* perceive benefits from using cloud computing has proven to be an important motive toward its adoption [52, 76]. Another effect of business partners is that they may require an enterprise to adopt cloud computing if they want to remain in collaboration with them [57]. Additionally, *competitors* play an effective role in incentivizing enterprises to adopt cloud computing for gaining market visibility, operation efficiency, and new business opportunities [23, 50]. This especially happens when the enterprise operates in a high-tech, rapidly changing industry [51, 52]. However, competitor pressure may not be relevant to SMEs, as they are more concerned about other cloud computing adoption issues such as cost reduction [51]. There is a lack of studies that explore the important role of the *cloud service broker* or the so-called service integrator in facilitating cloud computing adoption, with only one conceptual article, which described the G-Cloud program initiative in the UK. G-Cloud Authority is an internal cloud service broker that coordinates a managed and assured e-marketplace *CloudStore* of cloud services available to public sector organizations [71]. G-Cloud Authority eliminates the overhead for both cloud providers and consumers; the service makes it easy for cloud providers to sell cloud services, and enterprises do not need to spend a great deal of time in evaluating and selecting cloud providers [71]. The cloud service broker's role is to achieve a predictable end-to-end service outcome for enterprise users; this includes using standards for service management to predict, measure, and sustain cloud service outcomes [71]. Service management tools for cloud service brokers are available through the IT Infrastructure Library (ITIL); however, the ITIL is not mature enough yet [71]. The G-Cloud authority is responsible for providing cloud services once bought from the CloudStore, instantiating cloud services with appropriate business data, integrating the cloud service's management tools into the buying organization's service management

framework, and billing coordination [71]. Being commissioned by industry associations enhances the cloud-service brokerage's trustworthiness [71].

Internal Factors. These comprise the enterprise's internal characteristics and capabilities that affect its cloud computing adoption processes; these factors are: (1) willingness to invest, (2) top management, (3) firm size, (4) organizational culture, and (5) employees' IT skills. The enterprise's *willingness to invest* in and use cloud computing both financially and organizationally is claimed to be an important indicator for the adoption of cloud computing [23, 60]. Willingness can be affected by social influences (i.e., subjective norms and image), as enterprises would adopt cloud computing because its managers said cloud computing is a good thing and can enhance the enterprise's status among its social system [41]. Cloud computing adoption is also dependent on the role of the *top management*, as there is a relationship between top management innovativeness (i.e., adopt and accept new technologies) and the willingness to adopt cloud computing [45, 53, 88]. Top management's IT knowledge, competence, and capability of providing the suitable organizational climate for adopting cloud computing in terms of budget, adequate human and IT resources, and time [40, 45, 50, 51] is a cornerstone to the adoption of cloud computing. This involves: (1) understanding of cloud computing and its architecture, service models, and strategic values [23, 60, 67, 73, 81, 87]; (2) identifying enterprise's business needs and aligning IT decisions with business strategies [64, 83]; (3) evaluating the readiness of the existing IT infrastructure, IT knowledge, and skills of the human resources, available resources, and culture [23, 50, 60, 87]; and (4) holding the steering wheel toward cloud computing adoption (i.e., decide on adoption strategy, govern integration and implementation, and evaluate cloud services after use) with the guidance of external regulatory and professional bodies [49, 83].

Additionally, *firm size* is an important factor to cloud computing adoption [23, 50, 52, 56]. A study claims that if the company is spread over many countries, then it is likely controlling its own IT resource and does not need to adopt cloud services [81]. Further, a survey study conducted in Taiwan indicated that large enterprises are likely to adopt cloud computing [52]. On the contrary, a survey study in India indicated that SMEs can benefit the most [60], because large enterprises have sufficient resources to afford on premise solutions [50]. Another survey study reported that large enterprises are likely to proof concept of cloud computing services, and that SMEs can be more flexible in adopting cloud computing [53]. A conceptual article stated that SMEs are likely to be price-oriented and less concerned about performance, whereas large enterprises tend to balance costs against reliability, security, and performance [72].

Furthermore, *Organizational culture* is said to have an impact on the enterprise's adoption of cloud computing [49]. For enterprises that were used to the on premise approach and having full control over their data, it might be difficult for them to accept that the cloud provider will be fully controlling their data. Thus, enterprises would need to further ensure compliance of cloud computing solutions with the internal (i.e., corporate policies) and external (i.e., regulations and standards) constraints [49, 50, 83]. Therefore, culture, capabilities, and processes can be barriers to the realization of cloud computing benefits; thus, cloud service brokers can assist enterprises to overcome these barriers [71]. A survey study advocates the need to identify the way of thinking of organizational elements (i.e., staff, and management) regarding

culture that should be adjusted to meet the environmental needs and challenges in the future [47]. Further, *employees' IT skills* , especially non-IT employees', are said to be a crucial factor affecting cloud computing adoption decision, as their understanding of cloud computing is very important [23, 50, 52, 60]. Likewise, IT employees would have to adjust their skills to be able to use cloud solutions [49]. Another factor affecting cloud computing adoption decision is the enterprise's *prior experience* and familiarity with similar technologies, such as virtualization [51].

Cloud Computing Adoption Processes. These comprise processes that enterprises normally follow to adopt cloud computing along with the responsibilities and challenges faced in each process:

Evaluation. This comprises (1) costs and benefits, (2) impact on people and work practices, (3) internal readiness, and (4) cloud provider selection. Prior to cloud computing adoption, the top management is responsible for evaluating the enterprise's suitability for adopting cloud computing as well as the suitability of cloud computing for the enterprise [76, 81]. This includes: *evaluating the costs and benefits* associated with cloud computing in the long and short term, such as profitability, comparing the revenue generated from the firm's IT resources with the revenue expected from cloud computing, ROI, cost of migration and integration, cost of implementation, and hidden costs, such as support and disaster recovery [70, 80, 81]. *Evaluating the impact of cloud computing on people and work practices* is also a must [83], as it may change the role of IT staff and require them to acquire new skill sets (i.e., some jobs may be merged). Regarding the impact, chief information officers (CIOs) may feel they are at risk of losing relevance and, to overcome this, CIOs will need to contribute to business strategy and information management [71], which requires a change in culture and skills across the enterprise led by CIOs [71]. Further, cloud computing is argued to have a job relevance impact, that is, the extent to which cloud computing enhances the enterprise's status and day-to-day operations and provides services applicable to employees' jobs so that they have control over their work and complete their tasks quickly [42].

Evaluating the internal readiness of the enterprise, existing IT infrastructure and IT human resources, for adopting cloud computing [52]—in terms of having sufficient and reliable resources to support the use of cloud computing as well as appropriate learning routines and performance measures is argued to enable the adoption of cloud computing [42, 88]. *Selecting the cloud provider* based on the cloud provider's capability to provide robust security controls, the enterprise's understanding of issues related to the control over the data, the type of service model needed, and the perceived cloud provider's honesty, reputation, and sustainability [40, 65].

Proof of Concept. This comprises (1) trialability and (2) perceiving benefits and risks. *Trialability* is found to have a positive impact on the adoption of cloud computing [51]. Trying cloud services prior to the actual adoption to evaluate its applicability for the enterprise is likely to convince the enterprise to adopt cloud computing [76]. In this process, convincing enterprises to adopt cloud computing can be influenced by how they perceive cloud services. There is a wide agreement on the significant influence of the *perceived benefits and risks* on the adoption of cloud services [51, 86].

This is relatively in line with a survey study's findings that the management's perceptions of security, cost-effectiveness, and IT compliance are likely to have a significant impact on the decision to adopt cloud computing [63]. Cloud computing brings plenty of benefits that are relatively convincing for enterprises to adopt it. This includes cost savings, agility, flexibility, ease of use, scalability, facilitating collaboration between business partners, less operational effort on CIOs, and increased productivity [40, 50, 54, 64, 75, 76, 85].

Even with all these enticing benefits, some SMEs are still negative about adopting cloud computing services [51]. SMEs are concerned with various types of risks [54, 65, 68, 70, 76, 77, 86]:

- Organizational risks, which cover the risk of vendor lock-in as well as the loss of governance within the enterprise.
- Technical risks, which include data leakage, loss of data, downtime, data bottlenecks, and cyber-attacks.
- Legal risks, which include data protection regulations and licensing issues.
- Nontechnical risks, which refer to the misuse of cloud services and natural disasters.
- Performance risks, which are primarily that the moving of huge amounts of data to cloud servers takes a long time, and when moving further in the adoption, this will require increasing bandwidth and connectivity, which is costly [49].

Thus, benefits and risks perceived from trying cloud services will help enterprises to decide whether to adopt or not to adopt cloud computing.

Adoption Decision. This process comprises: (1) identifying business needs, (2) determining criticality, (3) evaluating strategic value, (4) implementation planning, (5) selecting the service model, (6) deploying model selection, and (7) contracting and SLA negotiation. When deciding to adopt cloud computing services, the top management is involved in the following activities: *evaluating core business needs* and competencies (i.e., quick response to market changes and increasing productivity) [61, 76], *determining criticality* in terms of what data and applications should move to the cloud (i.e., critical vs. noncritical data and applications) [69, 81, 82], *evaluating the strategic value* that cloud computing might bring to the enterprise, such as agility by delivering strong coordination IT capabilities, process management maturity, and reduced operational burden on CIOs so they can focus on strategic activities [75], *planning for implementation* of cloud computing systems in terms of the managerial time required to plan and implement cloud solutions was not problematic [60], whereas the problem was the planning for implementation of specific deployment models that suit the current applications [79]).

Furthermore, adoption decision process involves *selecting the right service model* (i.e., SaaS, PaaS, IaaS, or combined choice) that best fits the enterprise's needs [65, 66], *selecting deployment models* based on the sensitivity of the data and applications, if the data and applications are determined to be core, then they should be deployed on a private cloud, and if the applications are determined to be noncore, then they should be deployed on a public cloud [79], whereas another study suggests the core data and applications should not be deployed on the cloud at all [69]. Finally, the adoption decision is dependent on *negotiating the cloud service contract and SLA*

with the cloud provider, based on the sensitivity of the data [81], and reaching an agreement on [62, 65, 70, 71]: the modifications to the contract terms, description of services (cost, price, and service content), limitation on the use or reuse of the data, which includes the data sanitization policy to ensure that data are securely removed when the use of cloud services ceases, confidentiality and security requirements in terms of organizational standards for data encryption both at rest and in flight, risk management plans, indemnification, contract terms and renewal, effect of termination, ownership of the data and applications, location of the data, assurance of service availability and expected downtimes, employees access control and protective monitoring, and clarity on roles and responsibilities. These items should be discussed with the cloud provider before proceeding to implementation.

Implementation and Integration. These comprise (1) complexity and (2) compatibility. Compared to the on premise approach, cloud systems can be implemented and running in 24 hours instead of six months [49]. Thus, implementation of cloud systems is not problematic for enterprises, whereas integrating cloud systems with the enterprise's existing IT infrastructure can negatively impact their adoption of cloud computing [49]. Further, the use of cloud system by IT staff is straightforward, while it is challenging for the non-IT staff. This can be attributed to the degree of *complexity* of cloud systems in terms of the ease of understanding, use, and implementation or integration of cloud services. Although cloud computing is considered to be easy to understand and use, it arouses integration complexity issues [50].

Complexity is claimed to be a barrier to the adoption of cloud computing [23, 50, 52, 76]. Integration complexity problems emerge from the less standardized interoperability between cloud systems and the existing IT infrastructure, which triggers integration costs [50]. A survey study reported that the lack of legacy systems allows enterprises to implement cloud computing easily [42]. The lack of *compatibility* of cloud solutions with existing IT infrastructure can be a barrier to the adoption of cloud computing [52]. Interoperability standards can be an enabler or a barrier to the adoption of cloud computing [70]; they are enablers when the enterprise has its data, processes, and systems standardize priori, but as technology evolves, it becomes challenging for the enterprise to catch change in technology. Thus, the enterprise faces a challenge to integrate cloud solutions with already-existing cloud-based or traditional systems. In order to ensure desirable implementation and integration of cloud systems, IT governance initiatives are a required.

IT Governance. This comprises (1) auditability and traceability and (2) risk management. *Traceability and auditability* are cited to have impact on cloud computing adoption, and the former complements the latter [49]. The loss of IT governance within the enterprise can slow down the adoption rates because the data and applications are under the control of the cloud provider [65, 83]. Enterprises are advised to conduct audit trail meetings with the cloud provider to ensure a risk-free implementation of cloud solutions that complies with regulations, standards, and enterprise policies [49]. This is enabled by the top management through IT governance structures and processes [50]. Contrarily, IT governance processes in highly regulated industries will decelerate the adoption of cloud computing [50]. Further, IT governance processes might hinder the adoption if the integration of cloud solutions with the existing infrastructure appears to be difficult [50].

Despite the massive advancements in securing the cloud, security solutions are not tested extensively yet [81]. This matter could be dissolved by IT governance initiatives to ensure that enterprise policies, security standards, and legal requirements are met [49, 50]. Further, IT governance is attained by identifying responsibilities; for instance, the cloud provider may be responsible for the security at the IaaS level, whereas the customer's responsibility is at the SaaS and PaaS levels [83]. However, data security at the level of PaaS and IaaS service models can be a shared responsibility between the cloud provider and the adopting enterprise [66]. Additionally, cloud providers are required to provide traceable access controls to govern who can access what object under which conditions. This has to be validated by the top management for its conformity to internal and external constraints [49]. These controls are used to ensure data integrity and confidentiality [49, 65].

In regard to *risk management* during the planning for cloud computing implementation, a study suggests that the enterprise should consider evaluating the risk of storage damage, data loss, and network security [62]. For instance, the enterprise would maintain an on-site backup of the data moved to the cloud [69]. There is a lack of processes and methodologies that provides guidelines on how to use cloud services to address specific business needs and mitigate associated risks [71]. Eventually, securing enterprise's information from potential risks is more than processes, technical solutions, and people; it is an enterprise-wide security strategy to orchestrate these various elements [63].

Confirmation. This comprises *usage continuance*, about which a study proposed a model for implementation and confirmation stages of cloud computing adoption [79]. This study suggests the evaluation of cloud services based on the perceived attributes from using cloud services (i.e., relative advantage, complexity, compatibility, and trialability) to decide whether to continue using cloud services or not. Further, a survey study argued that perceived usefulness and satisfaction are necessary for IS continuance intention [43]. Apparently, satisfaction is not only related to perceived benefits from using cloud services, it is also dependent on the perception of service fairness from the cloud provider [43]. Service fairness happens when customers feel they are treated equally by the service provider as other customers are treated [43]. Thus, customers can judge how well-structured the cloud provider's system is, and, consequently, customers will likely continue to use the cloud provider's services [43].

4 Discussion and Future Research Avenues

This article sought to review 51 articles to capture the current state of IS research regarding cloud computing adoption in the context of enterprises. The review involved classifying the identified themes in the reviewed articles into cloud computing adoption factors and processes. The findings from the reviewed articles are discussed from three perspectives: theoretical (i.e., theories/frameworks/models utilized), methodological (i.e., research methods employed), and empirical (i.e., cloud computing adoption factors and processes). The contribution of this review is summarized in Fig. 2, where the identified cloud computing adoption factors and processes are depicted in addition to the relationships between them. In general, the review revealed

that only three IS journal articles were found contributing to the area of cloud computing adoption issues. Likewise, few IS conference articles appeared to contribute to the understanding of cloud computing adoption. In contrast, articles from non-IS journal and conference outlets are dominant in investigating this phenomenon. Based on the findings, a cloud computing adoption research agenda is drawn accordingly to direct research avenues to towards (1) theoretical, (2) methodological, and (3) empirical studies.

4.1 Theoretical Research Avenues

Articles utilizing the grounded classification and general concepts are dominant, whereas few already-existing theories were utilized to study the adoption of cloud computing. Yet, there is a need for applying more theories (e.g., institutional theory [90, 91]) that fit studying the adoption of IT innovation, to gain more insights regarding cloud computing adoption. Institutional theory captures the notion of irrationality in decision making, as enterprises may or may not adopt the cloud under internal (i.e., cultural resistance and internal readiness) or external pressure (i.e., competitors and business partners) and not because of efficiency and cost reduction. Moreover, institutional theory is helpful in understanding how enterprises respond to external and internal pressures and why [92, 93]. Consequently, this review brings interesting questions to IS researchers' empirical investigation briefcase: what factors (i.e., internal and external) affect the adoption of cloud computing, and how do enterprises form strategies to cope with these factors?

4.2 Methodological Research Avenues

The review indicates a lack of in-depth field and case studies regarding cloud computing adoption processes, as compared to those on cloud computing adoption factors, whereas the quantitative (i.e., surveys) studies and conceptual articles appeared to be dominant. Yet, there are theoretical studies that have not been tested. For instance, a study proposed theoretically a cloud computing adoption assessment model that considers criteria for selecting the cloud provider, but this model has not been tested empirically yet [67]. Thus, further qualitative research needs to be undertaken to explore further issues and test empirically the previous theoretical developments regarding this area.

Consequently, this triggers questions on the IS research round table as to why enterprises adopt cloud computing in spite of its potential risks? Or conversely, why enterprises do not adopt cloud computing in spite of its potential benefits? These questions need to be investigated thoroughly using multiple qualitative case studies in different contexts (i.e., countries and industries) to better understand cloud computing adoption factors and processes.

The majority of reviewed articles study cloud adoption factors and processes in a rather broad perspective. Therefore, there is a need for interpretive case studies to investigate each of cloud computing factors and processes found from this review (i.e., willingness, organizational culture, regulations, cloud providers trustworthiness, evaluation of cloud services, adoption decision, or implementation and integration processes) [94]. These in-depth studies are preferred owing to their implications for both practice and academia.

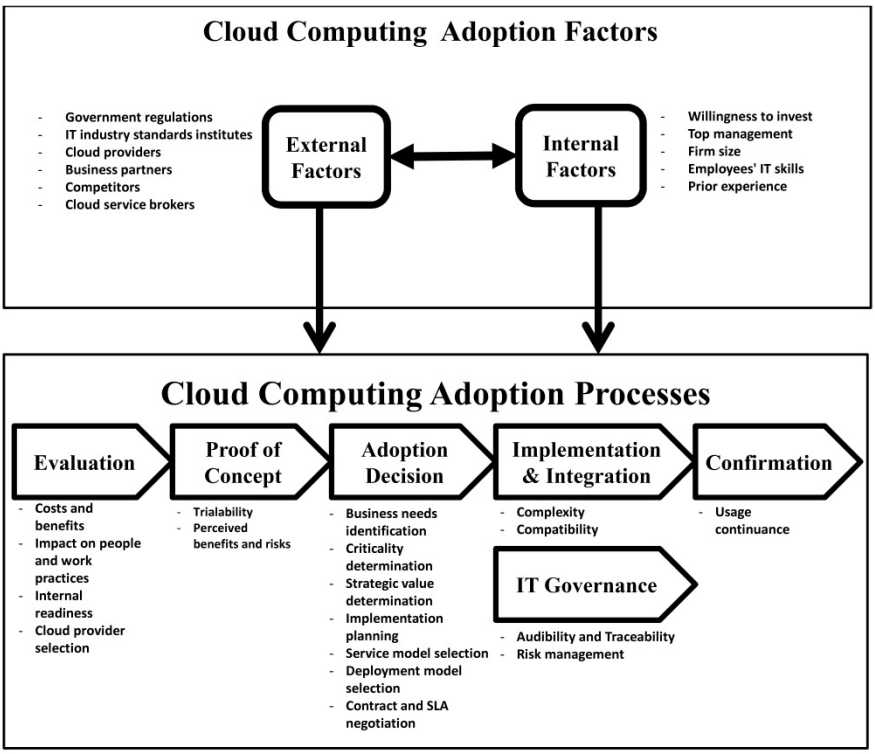


Fig. 2. Cloud computing adoption factors and processes

In spite of the appealing merits that cloud computing brings to enterprises (i.e., cost savings, flexibility, efficiency, agility and so forth), as an innovative IT shared services model [2], cloud computing puts enterprises in a decisive choice between on premise and on-demand approaches. In this regard, the Delphi method [95–97] would provide insights for IT managers about what are the most important issues, and their priorities, that should be considered when deciding to adopt cloud solutions. Further, this review advocates the need for conducting longitudinal studies to assess the impact of cloud computing implementation on both the technical and managerial capabilities of the enterprise (i.e., integration with existing IT infrastructure, planning, risk management, and IT governance) as well as the impact of the confirmation process on the organizational innovation.

4.3 Empirical Research Avenues

The review shows that cloud computing adoption processes received less attention from IS researchers in terms of exploring the challenges faced in each process and how enterprises cope with these challenges for risk-free adoption of cloud services. Legal issues are taking most of the attention in terms of the adequacy and consistency of government regulations for ensuring security and data privacy needed for using cloud computing services. In the developed world, these regulations, either national or

international, are in place, but they are inconsistent with each other, whereas, in the developing, world there is a lack of regulatory frameworks to assure safe adoption of cloud computing services. This implies the need for exploring cloud computing adoption in developing countries, as they may lack legal and IT infrastructures [78, 98], and the need for transferring lessons from the developed world to the developing one and vice versa.

According to the review, although cloud computing adoption factors have been investigated slightly more than the processes have, plenty of issues remain unclear. For instance, there is a conflict regarding the relationship between the firm's size and the likelihood to adopt cloud computing, and further in-depth studies are needed to address this conflict. Further, cloud computing is recognized as a cost-reduction solution; however, this cost reduction may not be significant, particularly in the context of SMEs, as reported by a survey study conducted in India [86]. Likewise, when the enterprise maintains an on premise backup, this adds to the cost as well [69]. If cloud computing helps enterprises reduce IT-related costs, then how significant will be this cost reduction be? Thus, further studies with focus on evaluating costs and benefits of cloud computing solutions would be favorable.

Moreover, there is a need for further exploring the impact of IT governance processes throughout the implementation process. There are still many legal (i.e., contract and SLA), ethical, and inter-organizational or institutional issues that need to be investigated regarding improvements of laws and standards. In addition, there is a need to explore the role of cloud service brokers in enabling cloud computing adoption and whether they have sufficient service management tools for provisioning cloud services or not. Moreover, trust issues are not addressed extensively in the reviewed articles, although it is claimed to be important for the successful adoption of cloud computing [3].

Further, it would be useful to investigate internal readiness and selection of cloud provider issues in the context of SMEs and/or large enterprises. Future studies should explore the compatibility between cloud solutions with enterprises' legacy systems and business needs, as well as the impact of trying or using cloud solutions on organizational culture, staff skills, and work practices. Another issue to consider is whether cloud computing releases enterprises from managing the IT infrastructure so they can focus on their core business activities, and if so, which data and applications should be moved to the cloud and which should remain in-house? Further studies would be appropriate for providing recommendations for practice regarding internal preparation, service model selection, and contract negotiation issues.

5 Conclusion

This study sought to conduct a systematic review of the extant literature on cloud computing adoption by enterprises. This involved identifying the current contributions of IS research regarding the phenomenon and determining the under-investigated issues and the contributions of IS research regarding the phenomenon. The classification of reviewed articles, findings, and implications for future IS research avenues are according to theories, research methods, and cloud computing adoption factors and processes that were identified by using GT approach. Yet, plentiful

legal, ethical, technical, and managerial issues are waiting for IS researchers to explore. Thus, the paper suggested a future IS research agenda based on the discussed findings.

This article is not free of limitations; it sought to review only academic articles from seven literature databases, leaving out white papers, magazine articles, other scholarly literature databases, and articles from a forward and backward search, the inclusion of which would help capture more issues about cloud computing adoption by enterprises. The search criterion was limited to article title only; however, including abstracts as a criterion would have revealed more insightful articles. The search phrases were limited; as some articles discuss cloud computing adoption using different words (i.e., utility computing or application service provision) that may not have been included in the search results of this review.

Acknowledgements. This paper is made possible through the help and support from Dr. Eli Hustad, Prof. Dag H. Olsen, Prof. Peter Axel Nielsen, and my colleagues Moutaz Haddara, Fathul Wahid, and Christoph Merschbrock. I owe them thanks for offering valuable advices on the logic and organization of the paper at its early stages. Finally, I sincerely thank the anonymous reviewers for their constructive advices that made the paper appear in a well-presented final shape.

References

1. Elragal, A., Haddara, M.: The Future of ERP Systems: Look Backward Before Moving Forward. Procedia Technol. 5, 21–30 (2012)
2. Su, N., Akkiraju, R., Nayak, N., Goodwin, R.: Shared Services Transformation: Conceptualization and Valuation from the Perspective of Real Options. Decis. Sci. 40, 381–402 (2009)
3. Garrison, G., Kim, S., Wakefield, R.L.: Success Factors for Deploying Cloud Computing. Commun. ACM. 55, 62–68 (2012)
4. Parakala, K., Udhas, P.: The Cloud Changing the Business Ecosystem (2011), http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/The_Cloud_Changing_the_Business_Ecosystem.pdf
5. Herhalt, J., Cochrane, K.: Exploring the Cloud: A Global Study of Governments' Adoption of Cloud (2012), http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/Exploring-the-Cloud.pdf
6. Venters, W., Whitley, E.A.: A Critical Review of Cloud Computing: Researching Desires and Realities. J. Inf. Technol. 27, 179–197 (2012)
7. RightScale: RightScale State of the Cloud Report (2013), https://www.rightscale.com/pdf/rightscale-state-of-the-cloud-report-2013.pdf
8. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: Above the Clouds A Berkeley View of Cloud Computing (2009)
9. Sultan, N.A.: Reaching for the "Cloud": How SMEs Can Manage. Int. J. Inf. Manage. 31, 272–278 (2011)
10. Yang, H., Tate, M.: A Descriptive Literature Review and Classification of Cloud Computing Research. Commun. Assoc. Inf. Syst. 31 (2012)
11. Cummings, M.P., Huskamp, J.C.: Grid Computing. Educ. Rev. 40, 116–117 (2005)

12. Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., Stößer, J.: Cloud Computing – A Classification, Business Models, and Research Directions. Bus. Inf. Syst. Eng. 1, 391–399 (2009)
13. EMA: Hybrid IT Service Management: A Requirement for Virtualization and Cloud Computing (2012), http://www.thinkhdi.com/~/media/HDICorp/Files/White-Papers/whtppr-FrontRange-Hybrid-ITSM.pdf
14. Heiser, J., Nicolett, M.: Assessing the Security Risks of Cloud Computing (2008)
15. Hashemi, S.M., Bardsiri, A.K.: Cloud Computing Vs. Grid Computing. ARPN J. Syst. Softw. 2, 188–194 (2012)
16. Susarla, A., Barua, A., Whinston, A.: Understanding the Service Component of Application Service Provision: An Empirical Analysis of Satisfaction with ASP Services. MIS Q. 27, 91–123 (2003)
17. Kern, T., Willcocks, L.P., Lacity, M.C.: Application Service Provision Risk Assessment and Mitigation. MIS Q. Exec. 1, 113–126 (2002)
18. Robison, S.: Everything-as-a-Service: A Blue Sky View of the Cloud (2009), http://www.hp.com/hpinfo/initiatives/eaas/SR_EaaS_viewpoint.pdf
19. Xin, L., Song, C.: Cloud-Based Innovation of Internet Long Tail. In: The 6th International Conference on Product Innovation Management (ICPIM 2011), pp. 603–607 (2011)
20. Kunesch, U., Reti, M., Pauly, M.: Cloud Computing I. Alternative sourcing Strategy for Business ICT (2010), http://www.t-systems.com/news-media/white-papers/760948_2/blobBinary/White-Paper_Cloud-Computing-I.pdf
21. Mell, P., Grance, T.: The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
22. Hogan, M., Liu, F., Sokol, A., Tong, J.: NIST Cloud Computing Standards Roadmap (2011), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909024
23. Espadanal, M., Oliveira, T.: Cloud Computing Adoption by Firms. In: Proceedings of the Mediterranean Conference on Information Systems, MCIS 2012 (2012)
24. Yang, H., Jing, S., Wang, H.: The Research on ASP-based SMEs Collaborative Platform. In: Proceedings of the 8th International Conference on Computer Supported Cooperative Work in Design, vol. 2, pp. 6–9 (2004)
25. Malathi, M.: Cloud computing Concepts. In: 2011 3rd International Conference on Electronics Computer Technology (ICECT), pp. 236–239 (2011)
26. Salleh, S.M., Teoh, S.Y., Chan, C.: Cloud Enterprise Systems A Review of Literature and its Adoption. In: Proceedings of the Pacific Asia Conference on Information Systems, PACIS 2012 (2012)
27. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., Ghalsasi, A.: Cloud computing — The Business Perspective. Decis. Support Syst. 51, 176–189 (2011)
28. Timmermans, J., Stahl, B.C., Ikonen, V., Bozdag, E.: The Ethics of Cloud Computing: A Conceptual Review. In: Proceedings of the Second International Conference on Cloud Computing Technology and Science, pp. 614–620. IEEE (2010)
29. Webster, J., Watson, R.: Analysing the Past to Prepare for the Future: Writing a Literature Review. MIS Q. 26, xiii–xxiii (2002)
30. Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: The 17th European Conference on Information Systems (ECIS 2009), Verona, Italy, pp. 2206–2217 (2009)

31. Levy, Y., Ellis, T.J.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Sci. J. 9, 181–212 (2006)
32. Dubey, A., Wagle, D.: Delivering Software as a Service (2007)
33. Okoli, C., Schabram, K.: A Guide to Conducting a Systematic Literature Review of Information Systems Research. Sprouts Work. Pap. Inf. Syst. 10 (2010)
34. Orlikowski, W.J., Baroudi, J.J.: Studying Information Technology in Organizations: Research Approaches and Assumptions. Inf. Syst. Res. 2, 1–28 (1991)
35. Galliers, R.D., Land, F.F.: Choosing Systems Appropriate Research Information Methodologies. Commun. ACM. 30, 900–902 (1987)
36. Gonzalez, R., Dahanayake, A.: A Concept Map of Information Systems Research Approaches. In: Proceedings of the IRMA International Conference, pp. 845–849 (2007)
37. Glaser, B.G., Strauss, A.L.: The Discovery of Grounded Theory: Strategies for Qualitative Research. Aldine Publishing Company, Chicago (1967)
38. Wolfswinkel, J.F., Furtmueller, E., Wilderom, C.P.M.: Using Grounded Theory as a Method for Rigorously Reviewing Literature. Eur. J. Inf. Syst. 22, 45–55 (2011)
39. Rich, P.: Inside the Black BoxRevealing the Process in Applying a Grounded Theory Analysis. Qual. Rep. 17, 1–23 (2012)
40. Bharadwaj, S.S., Lal, P.: Exploring the Impact of Cloud Computing Adoption on Organizational Flexibility: A Client Perspective. In: Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM 2012), pp. 121–131. IEEE (2012)
41. Opitz, N., Langkau, T.F., Schmidt, N.H., Kolbe, L.M.: Technology Acceptance of Cloud Computing: Empirical Evidence from German IT Departments. In: Proc. 45th Hawaii Int. Conf. Syst. Sci. (HICSS 2012), pp. 1593–1602 (2012)
42. Tjikongo, R., Uys, W.: The Viability of Cloud Computing Adoption in SMME's in Namibia. In: Proceedings of IST-Africa Conference, pp. 1–11 (2013)
43. Lawkobkit, M., Speece, M.: Integrating Focal Determinants of Service Fairness into Post-Acceptance Model of IS Continuance in Cloud Computing. In: Proc. 11th Int. Conf. Comput. Inf. Sci. (2012 IEEE/ACIS), pp. 49–55 (2012)
44. Shin, J., Jo, M., Lee, J., Lee, D.: Strategic Management of Cloud Computing Focusing on Consumer Adoption Behavior. IEEE Trans. Eng. Manag., 1–9 (2013)
45. Lian, J.-W., Yen, D.C., Wang, Y.-T.: An Exploratory Study to Understand the Critical Factors Affecting the Decision to Adopt Cloud Computing in Taiwan Hospital. Int. J. Inf. Manage. 34, 28–36 (2014)
46. Bogataj, K., Pucihar, A.: Business Model Factors Influencing Cloud Computing Adoption Differences in Opinion. In: Proceedings of the BLED 2013, pp. 1–14 (2013)
47. Kusnandar, T., Surendro, K.: Adoption Model of Hospital Information System Based on Cloud Computing Case Study on Hospitals in Bandung City. In: Proceedings of the International Conference on ICT for Smart Society, pp. 1–6 (2014)
48. Saedi, A., Iahad, N.A.: An Integrated Theoretical Framework for Cloud Computing Adoption by Small and Medium-sized Enterprises. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2013), pp. 1–12 (2013)
49. Morgan, L., Conboy, K.: Factors Affecting the Adoption of Cloud Computin An Exploratory Study. In: Proceedings of the 21st European Conference on Information Systems, pp. 1–13 (2013)
50. Borgman, H.P., Bahli, B., Heier, H., Schewski, F.: Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. In: Proceedings of the 46th Hawaii International Conference on System Sciences, pp. 4425–4435. IEEE (2013)

51. Alshamaila, Y., Papagiannidis, S.: Cloud computing Adoption by SMEs in the North East of England: A Multi-perspective Framework. J. Enterp. Inf. Manag. 26, 250–275 (2013)
52. Low, C., Chen, Y., Wu, M.: Understanding the Determinants of Cloud Computing Adoption. Ind. Manag. Data Syst. 111, 1006–1023 (2011)
53. Alshamaila, Y., Papagiannidis, S., Stamati, T.: Cloud Computing Adoption in Greece. In: Proceedings of UK Academy for Information Systems Conference, pp. 1–17 (2013)
54. Nkhoma, M.Z., Dang, D.P.T., De Souza-daw, A.: Contributing Factors of Cloud Computing Adoption A Technology- Organisation-Environment Framework Approach. In: Proceedings of the European Conference on Information Management & Evaluation, pp. 180–189 (2013)
55. Saedi, A., Iahad, N.A.: Developing an Instrument for Cloud Computing Adoption by Small and Medium-sized Enterprises. In: Proceedings of the International Conference on Research and Innovation in Information Systems (ICRIIS 2013), pp. 481–486. IEEE (2013)
56. Chang, B.-Y., Hai, P.H., Seo, D.-W., Lee, J.-H., Yoon, S.H.: The Determinant of Adoption in Cloud Computing in Vietnam. In: Proceedings of the International Conference on Computing, Management and Telecommunications (ComManTel 2013), pp. 407–409. IEEE (2013)
57. Cegielski, C.G., Jones-Farmer, L.A., Wu, Y., Hazen, B.T.: Adoption of Cloud Computing Technologies in Supply Chains: An Organizational Information Processing Theory Approach. Int. J. Logist. Manag. 23, 184–211 (2012)
58. Yang, C., Hwang, B., Yuan, B.J.C.: Key Consideration Factors of Adopting Cloud Computing for Science. In: Proceedings of the 4th International Conference on Cloud Computing Technology and Science, pp. 597–600 (2012)
59. Stankov, I., Miroshnychenko, Y., Kurbel, K.: Cloud Computing Adoption in German Internet Start-up Companies. In: Proceedings of BLED Conference, BLED 2012 (2012)
60. Rath, A., Mohapatra, S., Kumar, S., Thakurta, R.: Decision Points for Adoption Cloud Computing in Small, Medium Enterprises (SMEs). In: Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST 2012), pp. 688–691 (2012)
61. Abokhodair, N., Taylor, H., Hasegawa, J., Mowery, S.J.: Heading for the Clouds? Implications for Cloud Computing Adopters. In: Proceedings of the 18th Americas Conference on Information Systems, AMCIS 2012 (2012)
62. Tsai, C., Lin, U.-C., Chang, A.Y., Chen, C.-J.: Information Security Issue of Enterprises Adopting the Application of Cloud Computing. In: Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management (NCM 2010), pp. 645–649 (2010)
63. Opala, O.J., Rahman, S.(Shawon)M.: An Exploratory Analysis of the Influence of Information Security on the Adoption of Cloud Computing. In: Proceedings of the 2013 8th International Conference on System of Systems Engineering, pp. 165–170 (2013)
64. Subramanian, B.: The Disruptive Influence of Cloud Computing and its Implications for Adoption in the Pharmaceutical and Life Sciences Industry. J. Med. Mark. Device, Diagnostic Pharm. Mark. 12, 192–203 (2012)
65. Onwudebelu, U., Chukuka, B.: Will Adoption of Cloud Computing Put the Enterprise at Risk? In: Proceedings of the 4th International Conference on Adaptive Science & Technology (ICAST 2012), pp. 82–85. IEEE (2012)

66. Bamiah, M., Brohi, S., Chuprat, S., Ab Manan, J.: A Study on Significance of Adopting Cloud Computing Paradigm in Healthcare Sector. In: Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM 2012), pp. 65–68. IEEE (2012)
67. Nasir, U., Niazi, M.: Cloud Computing Adoption Assessment Model (CAAM). In: Proceedings of the 12th International Conference on Product Focused Software Development and Process Improvement, pp. 34–37 (2011)
68. Jensen, M., Schwenk, J., Bohli, J.-M., Gruschka, N., Iacono, L.L.: Security Prospects Through Cloud Computing by Adopting Multiple Clouds. In: Proceedings of the 4th International Conference on Cloud Computing (CLOUD), pp. 565–572. IEEE (2011)
69. Kim, W., Kim, S.D., Lee, E., Lee, S.: Adoption Issues for Cloud Computing. In: Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services - iiWAS 2009, p. 2. ACM Press, New York (2009)
70. Avram, M.G.: Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Procedia Technol. 12, 529–534 (2014)
71. Bellamy, M.: Adoption of Cloud Computing Services by Public Sector Organisations. In: Proceedings of the IEEE 9th World Congress on Services, pp. 201–208. IEEE (2013)
72. Kushida, K.E., Murray, J., Zysman, J.: Diffusing the Cloud: Cloud Computing and Implications for Public Policy. J. Ind. Compet. Trade. 11, 209–237 (2011)
73. Rawal, A.: Adoption of Cloud Computing in India. J. Technol. Manag. Grow. Econ. 2, 65–78 (2011)
74. Coursaris, C.K., van Osch, W., Sung, J.: A "Cloud Lifestyle": The Diffusion of Cloud Computing Applications and the Effect of Demographic and Lifestyle Clusters. In: Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS 2013), pp. 2803–2812. IEEE (2013)
75. Malladi, S., Krishnan, M.S.: Cloud Computing Adoption and its Implications for CIO Strategic Focus – An Empirical Analysis. In: Proceedings of 33rd International Conference on Information Systems (ICIS 2012), pp. 1–19 (2012)
76. Lin, A., Chen, N.-C.: Cloud Computing as an Innovation: Percepetion, Attitude, and Adoption. Int. J. Inf. Manage. 32, 533–540 (2012)
77. Nuseibeh, H.: Adoption of Cloud Computing in Organizations. In: Proceedings of the 17th Americas Conference on Information Systems, AMCIS 2011 (2011)
78. Bhat, J.M.: Adoption of Cloud Computing by SMEs in India: A study of the Institutional Factors. In: Proceedings of the 19th Americas Conference on Information Systems, pp. 1–8 (2013)
79. Dargha, R.: Cloud Computing From Hype to Reality. Fast Tracking Cloud Adoption. In: Proceedings of the International Conference on Advances in Computing, Communications, and Informatics, pp. 440–445 (2012)
80. Hoe, S.C., Kantarcioglu, M., Bensoussan, A.: Studying Dynamic Equilibrium of Cloud Computing Adoption with Application of Mean Field Games. In: Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 220–224. IEEE (2012)
81. Misra, S.C., Mondal, A.: Identification of a Company's Suitability for the Adoption of Cloud Computing and Modelling its Corresponding Return on Investment. Math. Comput. Model. 53, 504–521 (2011)
82. Kantarcioglu, M., Bensoussan, A., Hoe, S.C.: Impact of Security Risks on Cloud Computing Adoption. In: Proceedings of the 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 670–674. IEEE (2011)

83. Mcgeogh, B.T., Donnellan, B.: Factors That Affect the Adoption of Cloud Computing for an Enterprise A Case Study of Cloud Adoption Within Intel Corporation. In: Proceedings of the 21st European Conference on Information Systems, pp. 1–13 (2013)
84. Zhao, F., Gaw, S.D., Bender, N., Levy, D.T.: Exploring Cloud Computing Adoptions in Public Sectors: A Case Study. GSTF J. Comput. 3 (2013)
85. Gupta, P., Seetharaman, A., Raj, J.R.: The Usage and Adoption of Cloud Computing by Small and Medium Businesses. Int. J. Inf. Manage. 33, 861–874 (2013)
86. Iyer, E.K., Krishnan, A., Sareen, G., Panda, T.: Analysis of Dissatisfiers That Inhibit Cloud Computing Adoption Across Multiple Customer Segments. In: Proceedings of the European Conference on Information Management & Evaluation, pp. 145–152 (2013)
87. Luoma, E., Nyberg, T.: Four Scenarios for Adoption of Cloud Computing in China. In: Proceedings of the European Conference on Information Systems, ECIS 2011 (2011)
88. Khanagha, S., Volberda, H., Sidhu, J., Oshri, I.: Management Innovation and Adoption of Emerging Technologies: The Case of Cloud Computing. Eur. Manag. Rev. 10, 51–67 (2013)
89. Kihara, T., Gichoya, D.: Adoption and Use of Cloud Computing in Small and Medium Enterprises in Kenya. In: Proceedings of IST-Africa Conference, pp. 1–12 (2013)
90. Mignerat, M., Rivard, S.: Positioning the Institutional Perspective in Information Systems Research. J. Inf. Technol. 24, 369–391 (2009)
91. Weerakkody, V., Dwivedi, Y.K., Irani, Z.: The Diffusion and Use of Institutional Theory: A Cross-disciplinary Longitudinal Literature Survey. J. Inf. Technol. 24, 354–368 (2009)
92. Oliver, C.: Strategic Responses to Institutional Processes. Acad. Manag. Rev. 16, 145–179 (1991)
93. Deephouse, D.L., Suchman, M.: Legitimacy in Organizational Institutionalism. In: Greenwood, R., Oliver, C., Suddaby, R., Sahlin, K. (eds.) The SAGE Handbook of Organizational Institutionalism, pp. 49–77. SAGE Publications Ltd., Thousand Oaks (2008)
94. Walsham, G.: Interpretive Case Studies in IS Research Nature and Method. Eur. J. Inf. Syst. 4, 74–81 (1995)
95. Dalkey, N.C.: The Delphi Method: An Experimental Study of Group Opinion. In: Dalkey, N.C. (ed.) Studies in the Quality of Life: Delphi and Decision-Making, p. 161. Lexington Books (1972)
96. Okoli, C., Pawlowski, S.D.: The Delphi Method as a Research Tool An Example, Design Considerations and Applications. Inf. Manag. 42, 15–29 (2004)
97. Hsu, C., Sandford, B.A.: The Delphi Technique: Making Sense of Consensus. Pract. Assessment, Res. Eval. 12, 1–8 (2007)
98. Greengard, S.: Cloud Computing and Developing Nations. Commun. ACM 53, 18 (2010)

The Start of a Journey to The Cloud in The Developing World: A Case Study of Egypt

Rania Fahim El-Gazzar
Department of Information Systems, University of Agder, Kristiansand, Norway
rania.f.el-gazzar@uia.no

Abstract

Cloud computing (CC) is becoming a global market trend that all businesses, sooner or later, will go for. Moving to the cloud is a long journey for developing countries that became aware of its importance to their economic development. Egypt started this journey with collective efforts from all stakeholders (i.e., government institutes, national and international cloud providers, private businesses, and training institutes) to draw the roadmap for CC adoption in Egypt. CC adoption in Egypt is influenced by some enabling and inhibiting factors. These factors are explored by conducting an exploratory case study. The findings of this study are analyzed by utilizing concepts from the neo-institutional theory (i.e., isomorphic pressures and strategic responses to institutional processes). The findings indicate that factors enable or inhibit CC adoption in Egypt are variously associated to CC per se, limitations in developing countries in general, and Egyptian context in specific.

1. Introduction

Information and Communication Technology (ICT) is considered to play a key role in leveraging the socio-economic state of the developing countries [3,52]. CC is recognized by the United Nations as an evolving form of ICT landscape that has a considerable potential for social and economic development [19]. Thus, while the developing countries are experiencing social, economic, and political issues nowadays, they commenced thinking of CC to push their development wheel forward. The rationale is that CC, as an innovative model for delivering Information Technology (IT) services, brings about flexibility, scalability, efficiency, and cost-effectiveness to organizations [52]. However, developing countries are not, yet, harnessing such benefits from ICT innovations in the era of digital divide [3], as they lack the required technical, legal, and cognitive infrastructures to initiate their journey to CC [16,19,25].

Egypt has just started this journey by addressing its readiness for CC through a governmental initiative in 2011. This journey was disrupted by the Egyptian revolution, especially, on January 28th, 2011. That day was named "Friday of Anger" when all Internet connections and mobile phone communications were completely down by the government order and, thus, the public safety was threatened [39]. This made potential CC business users anxious. However, the government was determined to continue on its journey to the cloud.

In addition to the common limitations of developing countries towards adopting ICT innovations, Egypt is experiencing special political and social conditions that influenced the ICT strategy of Egypt negatively, but still there are positive efforts going forward. Perhaps the current situation of Egypt is temporary, but it might have short and long term impacts and it worth learning lessons from.

This paper tells about the Egyptian initiative towards CC adoption. Further, the paper presents a case study exploring enablers and inhibitors for enterprises' adoption of CC in the Egyptian context. The findings from the case study are analyzed by utilizing the neo-institutional theory, as thought to be insightful analytical lens [53], in attempt to answer the following research question: *How cloud computing adoption in Egypt is influenced by external pressures and why adopting organizations respond differently to such pressures?*

The remainder of this paper is organized as follows: Section 2 provides a background about CC in relation to developing countries in general and Egypt in specific. Section 3 provides a background on concepts from neo-institutional theory. Section 4 describes the Egyptian context and research method. Section 5 provides analysis of the findings. Section 6 discusses the findings. Section 7 concludes the contribution of the paper.

2. Background

CC reshaped the way IT services are delivered. This is evident from the definition of the National Institute of Standards and Technology (NIST) that CC is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [32:2].

1530-1605/15 $31.00 © 2015 IEEE
DOI 10.1109/HICSS.2015.520

NIST's definition implies that CC offers distinguishable capabilities such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [32]. Cloud Service Providers (CSPs) offer various service models depending on the level of control over the cloud infrastructure, while the basic ones are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [32]. These service models can be deployed in four models (i.e., private cloud, community cloud, public cloud, and hybrid cloud) to fit different needs and depending on the sensitivity of business data and applications [32]. CC offers several advantages to enterprises (i.e., agility by reducing IT operational costs and focusing on core business activities, innovation by scaling up and down the use of IT resources at no economic risk, etc.) [29,50].

2.1. Cloud computing in developing world

CC contributes to the socio-economic development of nations [24]; it helps developing countries to *leapfrog* the developed world [8]. Yet there are challenges to overcome in order for developing countries to realize the benefits from CC. In today's world of digital divide, where different societies experience inequalities in socio-economic conditions, ICT became a requirement for their economic and social uplift [2]. In this regard, CC is argued to offer a democratizing force for developing countries, whereas they could have an equal access to resources (i.e., hardware and software) as the developed countries have [46].

Through CC, developing countries can (1) grow in the global market and generate revenues (i.e., creating more business opportunities and leveraging local industries) [23,49], (2) improve government performance and public services (i.e., healthcare and education) [6,27,48], and (3) alleviate poverty (i.e., creating more job opportunities) [19]. Despite its enticing merits, CC is a double-edged sword. It raises some challenges that are attributed to CC per se and some others are related to the degree of the developing countries' readiness to adopt it (see Table 1).

There is a need for focusing research endeavors on the limitations related to developing countries that inhibit them from the ICT-driven development [3]. This entails exploring and addressing political, ethical, social, and cultural factors that impede developing countries from realizing the benefits of CC [25]. Furthermore, the use of theories is needed to understand how the socio-economic context enables or constrains the use of ICT innovations that improve life in developing countries [3]. This implies the need to study the role of political actors and institutions in providing basic infrastructures for ICT innovation and empowering societies [3]. Government institutes and IT industry associations are important for setting laws and standards, physically and financially supporting implementation of the IT infrastructure, and offering needed training programs [4,6]. Thus, collaboration with global partners helps dissolving limitations in developing countries and leveraging labor skills [8,26].

Table 1: Cloud computing challenges

Challenges	Description	References
Specific to CC	• Security controls and data privacy • Vendor lock-in that incurs switching costs • Uncertainty regarding CSP's liability (i.e., reputation and fate sharing) • No-gain risk (i.e., reduced capital and operative costs may not be sufficient enough to move from legacy systems to cloud platforms), • Compliance • Unclear cloud service performance parameters	[22], [29]
Specific to the context of developing countries	• Lack of basic IT infrastructure (i.e., connectivity and bandwidth) • Dependency on local power supplies • Lack of access to latest hardware and software • Lack of suitable legal rules and cloud specific policies • Lack of awareness of cloud benefits and risks • Lack of IT skills • Financial constraints	[4], [16], [25], [46]

Collaboration also creates a good relationship between stakeholders allowing knowledge exchange and innovation to better understand customers' business needs, improve CSPs' performance, and embed trust-generating networks [48]. Furthermore, usefulness, subjective norms, and advantages can affect the adoption of a particular technology such as CC; this manifests in the form of political, societal, economical, and technical trends [28].

2.2. Cloud computing in Egypt

There is a limited body of literature found exploring opportunities for adopting CC in Egypt. The manifestations of CC in Egypt appeared in the literature are web-based education, e-government, and social networking. In the area of web-based education, a survey study has been conducted in the British University in Egypt (BUE) to assess the effectiveness of using open source Moodle e-learning platform on improving the quality of students' comprehension, which is positively proved [1].

For cloud e-government in Egypt, a study argued that the transition of e-government to CC is not easy and has to be thoughtful; thus, the study proposed a "Before Cloud E-government" model or BCE-government model; this model consists of five stages for the transition of Egyptian e-government to CC: assessment, architecture re-construction, classification of services, aggregation, and legal contract [35].

Another study proposed a hybrid model for adapting e-government to CC in Egypt to minimize security, privacy, reliability, performance, and legal concerns [18]. This model consists of three clouds: (1) Intra-cloud that is a private cloud dedicated to a single national entity cluster, (2) Extra-cloud that is a community cloud that enables entities from different clusters to integrate and aggregate their work as required, and (3) Inter-cloud that is a public cloud that enables users (i.e., citizens, guests, or organizations) to communicate with the government entities.

With 16 million Facebook users, Egypt constitutes about a quarter of total Facebook users in the Arab region and 1.4% of global Facebook users; this ranks Egypt as first among the Arab region and 17th worldwide [41], [15]. Twitter users in Egypt are small, approximately 519,000 users, compared to their Facebook equivalents [40]. Egyptian youth used Facebook and Twitter to lead the first cyber revolution in January 25th, 2011 to take down president Mubarak and change his regime [39]. The use of social media for such political reform had impact on political, social, and business spheres in Egypt. Further, Mubarak's government reactions to the revolution had negative impact on ICT industry in Egypt in general, and CC in specific [39]. However, the new government is dedicating efforts to turn this negative impact into a positive one and leverage Egypt's image worldwide.

3. Neo-institutional theory perspective

CC as an innovative IT sourcing model [44], its adoption is influenced by various factors (i.e., political, economic, normative, social, and cognitive). Neo-institutional theory is felt to be insightful analytical lens for providing causal explanations [17]. Neo-institutional theory is appropriate for examining IT adoption and use [34], understanding the influence of institutions on the use and consequences of technologies [37], and studying ICT for development issues in the developing world [51].

The central construct of neo-institutional theory is the *organizational field* that forms a community of organizations (i.e., government, CSPs, business partners, and IT industry associations). These organizations enact and reproduce *institutions* to shape the adoption of IT [42]. These institutions are carried through symbolic systems (i.e., rules, laws, and values), relational systems (i.e., governance systems and authority systems), routines (i.e., protocols, standard procedures, and roles), or artifacts (i.e., objects that comply with standards) [43]. Institutions impose three isomorphic pressures on the adopting organizations, so that they look similar to each other (see Table 2) [10]. To respond to these isomorphic pressures, organizations enact five strategies expressed through tactics in order to gain, maintain, or repair their legitimacy (see Table 3) [36,45]. These strategic responses are enacted for the sake of gaining *Legitimacy*. Legitimacy is defined as the 'congruence between the social values associated with or implied by [organizational] activities and the norms of acceptable behavior in the larger social system' [11:122].

Table 2: Isomorphic pressures [10]

Isomorphic pressures	Description	Sources
Coercive	Formal (standards) Informal (culture)	- Legal environment
Normative	Normative rules about organizational and professional behavior. Producing individuals with similar orientation and educational backgrounds.	- Professional associations - Universities and professional training institutions
Mimetic	When organizations are confronted with poorly understood technology solutions, ambiguous goals, and environment uncertainty, they model themselves on other organizations in hope to find less expensive solutions.	- Consulting firms - Industry trade associations - Employee transfer or turnover (implicit)

Table 3: Strategic responses to isomorphic pressures [36]

Strategic responses	Tactics	Description
Acquiescence	Habit	Following invisible, taken-for-granted norms
	Imitate	Mimicking institutional models
	Comply	Obeying rules and accepting norms
Compromise	Balance	Balancing the expectations of multiple constituents Negotiating with institutional stakeholders
	Pacify	Placating and accommodating institutional elements
	Bargain	Negotiating with institutional stakeholders
Avoidance	Conceal	Disguising nonconformity
	Buffer	Loosening institutional attachments
	Escape	Changing goals, activities, or domains
Defiance	Dismiss	Ignoring explicit norms and values
	Challenge	Contesting rules and requirements
	Attack	Assaulting the sources of institutional pressure
Manipulation	Co-opt	Importing influential constituents
	Influence	Shaping values and criteria
	Control	Dominating institutional constituents and processes

4. Context and research method

4.1. Context

In recent years, ICT sector was given a considerable attention from the Egyptian government, as it significantly contributes to the growth of Egypt's economy [31]. Ministry of Communications and Information Technology (MCIT) promoted the use of ICT for the development of Egypt through several national and regional initiatives with national and international partners; this aimed at providing

training programs, capacity building, exchange of expertise, and sustainable development [31].

According to ICT Development Index (IDI) reports, Egypt recorded a ranking progress from 91st in 2010, 87th in 2011, to 86th in 2012 worldwide in terms of access, use, and skills of ICT [20,21]. According to Networked Readiness Index (NRI) reports, Egypt recorded a backward move in ranking from 74th in 2011, 79th in 2012, to 80th in 2013 in terms of having the environment for ICT, readiness to use ICT, actual use of ICT, and impact of ICT on economy and society [5,12,13]. However, a recent report indicated that Egypt is among the economies that meet minimum requirements for basic cloud services [19].

For Egypt, CC is "a technology priority which positively impacts the local economy in alignment with the global trend" [30:24]. However, this technological transition requires thoughtful initiatives in order for Egypt to be legitimate in the widely growing market of CC. Thus, CC is one of the strategic goals of Egypt's ICT strategy in the near and long future [30]. This manifested in the project initiative entitled "Supporting ITI Activities – Phase II" in 2011[1]. The responsible parties for this project are the Egyptian MCIT[2] as an implementing partner in collaboration with the Information Technology Institute (ITI)[3] in Egypt that operates by MCIT and the United Nations Development Programme (UNDP) as responsible parties. The motive for this project was the Egyptian government's belief that ICT plays an important role in leveraging the national economy and promoting innovativeness[2]. Thus, there was a need for capacity building to cope with the ever-changing nature of ICT industry in terms of market needs and job requirements. All this pours into enhancing Egypt's reputation as a global competitor[2].

The project targeted three outputs: (1) Promote innovation and entrepreneurship across ITI and private sector. (2) Enhance skills of Egyptian youth and create job opportunities. (3) Enhance ITI international cooperation. The first step in this initiative is that the ITI established the Egyptian Cloud Computing Center of Excellence (EC3)[4] as a public private partnership among ITI, academia, and industry to place Egypt as a credible cloud provider in the global CC market as well as involve Egypt in research and development to explore aspects of CC[2]. EC3 also provides Small and Medium Enterprises (SMEs) with IT resources to benefit from CC.

Second step was that the ITI will provide: (1) training for the staff of the EC3 and employees from private sector, and (2) 9-month professional program to develop IT skills of university graduates and arrange a job fairs event, where private companies are put in contact with these graduates for internship and job opportunities.

Third step involved promoting cooperation between the ITI and national, regional, and international stakeholders with purpose of sharing knowledge and experience among Egyptian and international professionals from organizations, training and legislative institutes, and universities. This cooperation takes place in "Cairo ICT" conference[5] through sessions, tutorials, and technology and business exhibitions. Cairo ICT conference is organized by the ITI in cooperation with the Institute of Electrical and Electronic Engineers (IEEE). A series of sessions, workshops, and panel discussions has been held in Cairo ICT conference in May 20th, 2013 under "cloud computing forum" theme. This event involved discussing with all stakeholders how CC is beneficial for Egypt and what challenges that the new Egyptian government has to address in order to pave the way to CC.

According to one of the panel sessions in this event, a series of working groups sessions are planned, under the auspices of MCIT, to communicate the CSPs and consulting firms representing expertise and potential adopters representing the 'needs', as CC adoption is going to be driven by these needs. One of the most critical issues in Egypt's journey to the cloud is the migration of business processes to the cloud, and potential adopters are cautious about it and need to gain knowledge about best practices and successful stories in migrating to the cloud in order to draw their roadmap. This is the national strategy for CC adoption, while the regional strategy involves having Egypt as a hub for CC in the Middle East region to provide public cloud services, as its geographical location is appealing.

4.2. Research method

Given the limited empirical research regarding CC adoption in the Egyptian context, an exploratory case study was conducted [54]. Case study is an appropriate method for addressing *how and why* questions [54]; it is useful for exploring areas where existing knowledge is limited [7]. Case study strategy is useful in understanding dynamics of the context of the phenomenon under investigation [9,54], and the human/technology interaction in the natural social setting [38].

This study is based on various data sources including 13 semi-structured interviews using different modes of communication, document and text analysis (i.e., reports generated by MCIT and news articles), and video recordings for events held by the MCIT regarding CC (i.e., Cairo ICT conference), to achieve triangulation [14]. The interviews are conducted with various stakeholders, who are chosen purposefully, including CSPs operated privately

[1] Collaboration project to promote innovation and entrepreneurship, develop professional calibers, and enhance international relations: http://www.undp.org/content/dam/undp/documents/projects/EGY/00060666/Pov_Pro%20Doc_ITI%20Phase%202.pdf

[2] http://www.mcit.gov.eg

[3] http://www.iti.gov.eg

[4] http://www.ec3-egypt.net

[5] http://www.cairoict.com

or by the government, cloud service brokers, and clients. Further, the interviewees are from different levels (i.e., managers, consultants, and software engineers).

5. Findings analysis

Cloud customers (i.e., government authorities and business companies) strive to gain legitimacy within both local and global markets by choosing various adoption strategies. In the context of Egypt, the community organizations in the surrounding organizational field are government authorities, CSPs, partners including government and non-government institutions both national and international, and industry standards associations. The findings from this study are arranged according to the isomorphic pressures imposed through institutions that are enacted by these community organizations (i.e., coercive, normative, and mimetic). Furthermore, a set of strategic responses to such pressures are explained (i.e., acquiescence, compromise, avoidance, defiance, and manipulation) and justified.

5.1. Isomorphic pressures

5.1.1. Coercive pressure. It can occur outside the governmental arena [10]; this includes vendor lock-in pressure that is exerted by CSPs, especially, when adopting SaaS service model. In this case, customer companies would either adhere to the CSP's standard operating procedures or incur the hassle of starting from scratch. A technical consultant works for a local CSP that provides cloud-based ERP explains the scenario of termination that they state in the SLA: *"If the customer doesn't want our ERP application anymore, we export the data using CB [Community Builder export] and the customer gets back the data in excel files with regular excel tables."*

According to an IT consultant viewpoint, it is not a problem to change from CSP to another at the level of PaaS and IaaS service models. Unlike the SaaS model, where the customer company will have to do the same thing all over again. An IT consultant stressed on this: *"….. a major problem of the cloud is the 'lock-in'….the easiest model is the IaaS, because you could buy a server from CSP and upload all your data on it….Unlike SaaS model, you worked with the CSP, explained your business logic, tested the application, and found bugs and fixed them. So, you wouldn't start over all this again!..."*

5.1.2. Normative pressure. Professional networks, training institutions, trace associations are sources of normative pressures [10]. By holding sessions, workshops, and panel discussions in Cairo ICT conference, the new government, in collaboration with partners (i.e., national and international cloud providers and other institutions) could impose a normative pressure to spread awareness among business companies and government authorities who are potential adopters of cloud services.

In the opening session of cloud computing forum event, the minister of CIT Dr. Atef Helmy stated that the purpose of MCIT is, first, to attract foreign investments with intention to create job opportunities for youth and, second, to stimulate the market and support companies that work in ICT sector. In this regard, he elaborated on the benefits of CC, and how it will be discussed in the event, saying: *"There are various CC business models will be discussed in detail, that offer competitive advantages for all users including large, small, and micro enterprises. This seminar will be followed by a number of workshops under the auspices of MCIT and run by participating partners from national and international companies to understand the potential of CC applications in the Egyptian market….I hope that all parties including national and international companies, ministries' representatives, or other institutions in all sectors collaborate together to achieve fruitful outcomes from this forum. I expect that this will result in absorbing experiences from international companies and gaining maximum benefits."*

Other manifestations of normative pressures are the training programs offered by the ITI for university graduates and private sector's employees. Furthermore, Technology Innovation and Entrepreneurship Center (TIEC) offers training courses and international certificates for business owners and technical professionals who want to enrich their knowledge about CC [30]. Standards provided for data security either by professional associations or CSPs themselves are also normative guidelines used, as indicated by a Technical Operation Manager, to protect the data. These include: ISO 27/1001, Microsoft Internet Security Acceleration (ISA) Server, and Payment Card Industry-Data Security Standard (PCI-DSS).

5.1.3. Mimetic pressure. This includes pressures exerted by global business trends, peer organizations, and consulting firms. Organizations model themselves to similar organizations in their field that are perceived to be more legitimate or successful and that innovation can be accounted for by organizational modeling [10]. In this regard, there are global (i.e., business trends) and local (i.e., peer organization) mimetic pressures affecting CC adoption in Egypt. CC became a global business trend, so that the Egyptian government and business companies strive to model themselves on this IT innovation to gain legitimacy within the global market. An IT consultant stressed on that: *"….sooner or later all companies will go cloud….the global business trend pressure will result in people moving to the cloud."* In this regard, the minister of CIT announced that CC will be widely applied in all sectors to legitimate the Egyptian market with the global market trends: *"Undoubtedly, CC is not only a global market trend, but it also offers special advantages, such that its applications would have positive impact on the government, large enterprises, and attracting more investments. Furthermore,*

it [CC] will be applied in all other sectors and I, especially, mention small, medium, and micro enterprises."

Peer organizations can exert a mimetic pressure by sharing their successful experience with an innovation or a practice. A technical consultant attended an event for Microsoft and told that the IT manager of the National Bank of Egypt (NBE) was speaking about the story of improving their IT infrastructure using CC: *"the IT manager of the NBE …..was talking about the cloud in an optimistic way and showing us that a bank is using the cloud!! Because we wouldn't believe it!!!!!"* They tested some of their business scenarios on Windows Server 2012 [33]. In a panel discussion about government and private cloud held in Cairo ICT cloud computing forum conference, the Chief Technology Officer (CTO) of Abu Dhabi Islamic Bank shared their positive experience with cloud technologies and he advocated other banks to start using cloud services.

Departing from the argument that models can diffuse through consulting firms [10], such firms may recommend certain strategies by which CC adoption would be reasonable. In alignment with this, an IT consultant stated a strategy that he would recommend to cloud customer companies, which is the test environment:*"… The niche of CC is that, if somebody is about to implement an IT solution and needs a test environment, I would tell them 'cloud is a must and you can have it immediately'….. It doesn't matter if the application is meant for financial data or something else because there won't be any data…. so there is no risk."* So, customer companies can benefit from CC as an immediate test environment for their applications.

The IT consultant also hinted an important point that he would recommend to potential cloud customers, that CC would be cheap in the case of dynamic loads: *"….unfortunately, the marketing media either inside or outside Egypt advocate the notion of "cloud is cheaper", while it is not cheap at all! But it solves many problems within enterprises. CC can be cheap in some situations..… If a dedicated hardware is bought for a dynamic load in a hectic period of special offers, this hardware won't be utilized the rest of the year!…cloud is easier and much cheaper in this case…"*

5.2. Strategic responses to isomorphic pressures

5.2.1. Acquiescence. Some customer companies follow imitation tactic by adopting public cloud services such as the Egyptian electricity holding company and Egyptian ambulance organization. A technical consultant, in a local CSP that provides cloud-based ERP solutions, mentioned their fine work experience with the Egyptian electricity holding company, branch of Behaira governorate, saying: *"We developed a cloud-based ERP for them. We worked for this company for a long time, through which they first asked us to develop a desktop application for them, and then they decided to use public cloud-based ERP."*

5.2.2. Compromise. Other customers follow bargaining tactic to negotiate with institutional stakeholders the best CC adoption strategy. This manifested in a panel discussion about government cloud held in Cairo ICT cloud computing forum conference with different stakeholders, wherein the director of information infrastructure sector in MCIT stressed on the need for two things: *"….[first] we need a regulator to regulate the matters in CC ranging from security, SLA …etc. Because without a regulator, CC will spread in a chaotic way…..[second] we need something called 'Gov. Store';…this Gov. Store holds cloud-based applications that conform to the regulator's security and SLA requirements, so that government authorities can use these applications according to their needs, instead of implementing a solution for each ministry or department in the government, which would take a long time!"*

Some other customer companies follow pacifying tactic by accommodating several institutional influences. This is the case of Telecom providers in Egypt who implement hybrid clouds; they implement their private clouds to become CSPs afterwards selling public cloud services according to an IT consultant's statement.

5.2.3. Avoidance. This manifests in concealing tactic, where customer companies disguise themselves to appear as adopting cloud services for the sake of proofing concept without full implementation, to demonstrate its feasibility. This is expressed by a SharePoint technical consultant *"……mostly, customers come to us to try cloud services and, until now, we didn't deal with customers who are going for full implementation. Even SharePoint from Microsoft that is a known worldwide,…..customers tend to try it first…"*

5.2.4. Defiance. This happened through a dismissing tactic, where customer companies both government authorities and private businesses in Egypt resist the idea of adopting public CC services and prefer to keep on their traditional IT solutions. This resistance is related to various concerns such as political uncertainty, limited connectivity, data security, resistance to change, and lack of awareness:

Political uncertainty. This resulted from the arbitrary decree from Mubarak's government in 28th of January 2011 to shut down the Internet [39]. A senior solution manager for a CSP said expressing customer companies' fears: *"…recently Egypt faced an Internet outage due to the decree from the government which is not accepted and we must have a law that prevents governments from forcing Internet providers to cut Internet services, as this becomes a very weak spot for cloud services trend in Egypt, all companies are now afraid from facing similar situation that their dependence on CC will lead to outage and will impact their business."* The government decree on the Internet providers to shut down the Internet caused unfavorable

influence on the way customer companies perceive CC; they perceive it as a threat to their business rather than an opportunity. This event will remain a crucial point in customers' heads when deciding to use cloud services.

This lack of trust requires an extreme effort from the new government to proof that this will not happen anymore. This led the new government to hold a series of meetings and sessions under Cairo ICT conference; this event is inaugurated with words from the Chief Executive Officer (CEO) of Trade Fairs International company speaking on behalf of the MCIT: *"… Egypt is currently going through economic and political situations that may not seem to be favorable, but in fact, we can say that with every great challenge comes a greater opportunity….. people are afraid and they have the right to be afraid, but our duty towards Egypt is to turn all these fears into fruitful hard work…and through ICT community, Egypt can face any challenges and attract investments."*

Limited connectivity. It is a common infrastructure problem in Egypt. This is stressed by a consulting system engineer saying: *"one of the reasons that can affect the use of cloud services in Egypt is the Internet speed and stability; it is slow and often goes down because of problems in the infrastructure in terms of cables and centrals."* Telecommunications infrastructure in Egypt is not sufficient enough for CC technology, but it provides the minimum for businesses to survive while using some cloud services. This is pointed out by a senior solution manager saying: *"Telecommunications infrastructure in Egypt currently is not powerful enough to switch a business to the cloud but at least it can handle 50 % of the needs to run a business in the cloud…."*

However, connectivity problem needs a radical solution from the Egyptian government. This is announced as a priority in the ICT strategy of Egypt by the minister of CIT in Cairo ICT conference: *"we have to work on a set of trajectories to provide the capable IT infrastructure (i.e., CC, broadband, and submarine communications cables) that enables us to boost the geographical position of Egypt as an international hub for the Internet and achieve socio-economic development for Egypt through ICT"*

Despite connectivity, that is the core ingredient for using cloud services, is not adequate, it is not catastrophic. Data security would be the most irritating concern. This point is stressed by an IT consultant: *"….the bandwidth is not sufficient as the other advanced countries; it is at the minimum….connectivity wouldn't be problem number one, but data security would be."*

Data security. Security is a showstopper for CC adoption in Egypt. CSPs offer various technical security solutions to encrypt data while at rest in the database or on transfer between servers, as well as list guarantee terms in the service contract; this seems to be not enough for customers to feel safe. Security fears still exist and can be attributed to cultural and legal issues.

Culture-related data security issues are referred to the common sense of not accepting the data to be off-premise; this is stressed by the account manager of multinational CSP, Egypt subsidiary, saying: *"….the problem in Egypt is mainly cultural. People share same concerns about 'my data should be with me'; it is like our Egyptian saying 'I would carry my son on my shoulders, rather than leaving him somewhere and looking for him afterwards.', although we encrypt the data at rest and on transfer and put firewalls. Additionally, we sign an agreement, through which we guarantee security of the data."*

The legal framework is completely absent in Egypt. There is a lack of government laws to govern the use of cloud services and manage the relationship between cloud customers and CSPs. This issue is stressed by a consulting system engineer works for a customer company:*"…unfortunately, the terminology SLA is not existing and all Egyptian CSPs do not provide cloud services at a satisfactory level; we used to this situation in Egypt, that no one cares anymore about the agreement between the customer and the service provider…"*

The hard truth is that the regulatory bodies in Egypt are existent but still inactive regarding CC and the only guarantee for data security and privacy is the conditions stated in the service contract. This is pointed out by an IT consultant: *"…. Unfortunately, there is no such thing! We have the entities responsible for enacting ICT regulations like MCIT and NTRA [National Telecommunication Regulatory Authority]. However, these entities haven't enacted any regulations for CC industry, while they should have like other countries already have! …in the U.S., it is prohibited to put healthcare data of American citizens outside the U.S. …Whilst in Egypt, nothing is prohibited or permitted; there are regulators but no regulations at all!.....business wise, if something wrong happened to the customer's data, any actions regarding such situation will depend on the terms and conditions that are stated in the contract between the customer and the CSP..."*

Egyptian government would only be concerned about consumer rights and data privacy issues of CC if it is a cloud customer. In this regard, a technical consultant in an Egyptian CSP stated that: *"…Government didn't reach the degree of maturity enough for engaging in legal matters…the government doesn't engage in how we should provide cloud services… until it becomes a cloud customer. Then, the government gets concerned about national security to protect their clients only. They don't apply consumer protection authority in cloud market yet."*

Resistance to change. Old generations seem to be reluctant towards CC than youth. This reluctance depends on the origins of the customer company. This is demonstrated by a consulting system engineer saying: *"…unfortunately, old generations either managers or regular employees are not easy to convince and often do not accept this technology [CC]. This could be attributed to*

the consequent change of adopting CC…..However, international companies that have subsidiaries in Egypt show more interest in adopting CC, hence, employees follow the policy of the company from outside Egypt…." Following on what he said, the change that CC entails can affect the roles of old generations, especially, managers and executives. This is pointed out by a managing consultant saying: *"CIOs and IT directors fear CC as it minimizes their own power in the enterprise drastically."*

Lack of awareness. A further reason for customers' resistance is the lack of deep knowledge about CC per se. CC term is fuzzy for the customers; they don't see clearly the benefits that CC will bring to them compared to traditional IT solutions. A senior solution manager reflected on that saying: *"Many companies in Egypt do not know the meaning of CC and what advantage they will get from using it ….they start to use virtualization technologies; however, virtualization is the main requirement for the cloud but does not mean that they are using cloud services…..they are still thinking with the traditional mind (My Servers and Systems must be on premises)…."* In this regard, a co-founder and manager of a CSP stated that they are about to start awareness campaigns.

5.2.5. Manipulation. Customer companies that work in critical industry (i.e., banks) tend to follow influence tactic by shaping criteria to implement their cloud; this includes privatizing their virtualized IT resources. As a senior solution manager stated that: *"…the Idea of private cloud is more acceptable for Egypt culture than public one….."* In one of the panel discussions in Cairo ICT cloud computing forum conference, the CTO of Abu Dhabi Islamic Bank stressed that the public cloud was almost impossible option to think about because of the regulations of banking industry and the guidelines of the central bank of Egypt, as the critical aspect in banking sector is the secrecy of the data. Thus, the private cloud was a literal choice for them. They started to look for cloud solutions that fit their critical requirements. They started determining what they want to do and what are the benefits from CC for their business as a bank. They started with their IT infrastructure then the applications and so on. They were trying to compete in their very dynamic environment; this required them to look for IT solutions that enable them to implement products and deploy applications rapidly.

A further challenge was that they didn't have a robust disaster recovery site, especially, during the Egyptian revolution and what they faced from disruptive events such as stealing communication lines. Thus, they needed to implement a firm disaster recovery site. With help from HP, Microsoft, and Citrix, they could transform their old traditional data center into a virtualized one in six months. Furthermore, they implemented cloud-based disaster recovery site up to the level of virtualization and they put all necessary security layers. Then, they could move all their work over night to the disaster recovery site. After telling their story, he shared some benefit they gained from their implementation of private CC model. In the old data center, they had 28 racks, while with the new setting of CC model they had 10 racks. This reduced power consumption significantly. Additionally, they could consolidate their servers by deploying 140 virtual servers on five physical servers.

6. Discussion

The findings from this study indicate that the journey to the cloud in Egypt is still in the beginning and, yet, there is more to do in order to become mature in this industry. This paper explored factors that affected the adoption of CC in Egypt. Furthermore, the paper provided an overview of the current state of CC adoption in Egypt. Table 4 provides a summary of the isomorphic pressures exerted to influence the adoption of CC in Egypt and the sources of each pressure. Table 5 provides a summary for various strategic responses to the isomorphic pressures with various tactics and justification for each strategic tactic.

CC is introduced newly in Egypt and its market is still not mature. There are missing pillars for its adoption to spread. However, some initiatives and efforts were dedicated to address challenges and realize opportunities from adopting CC in Egypt to leverage the socio-economic development of the country. CC adoption in Egypt is faced with many challenges and opportunities. Public cloud services are not widely adopted for security reasons; however, private clouds are favored among adopters as well as proofing concept. To conclude, factors influenced CC adoption in Egypt can be categorized into two categories (i.e., enabling and inhibiting).

Enabling factors to the adoption of CC in Egypt consist of (1) implementing EC3 as a credible CSP operating by the government, (2) holding sessions and workshops that gather all stakeholders to spread awareness, determine business needs, share knowledge and expertise, and showcase successful implementations of cloud models by peer organizations, (3) offering training programs to improve human resources' skills, (4) consulting firms, through which customers know what, how, and when to move to the cloud, and (5) the MCIT is considering an ICT strategy for expanding the broadband and submarine communications cables to provide the sufficient connectivity for CC service models. However, as CC adoption in Egypt is not mature yet, serious fears are stepping back some customer companies from adopting CC services.

Inhibiting factors to the adoption of CC in Egypt consist of (1) vendor lock-in, as the customer company has to start over the whole development cycle in case of changing the CSP; findings from the study show that the CSP delivers the data in excel files to the customer in case of contract termination. (2) political uncertainty manifested in distrusting that the Internet cut by the government will not

happen again, which would affect customers' business as CC is mainly dependent on the Internet, (3) limited connectivity is a common problem of the IT infrastructure in Egypt in terms of speed and stability, (4) data security concerns resulting from the mental culture of 'having own data on own site' and lack of legal framework, as regulators are in place but regulations are not, (5) resistance to change is obvious in managers from old generations and also this resistance results from the fear of eliminating the role of CIOs, and (6) lack of awareness about CC concepts and considering it as same as virtualization; additionally, customer companies do not know how good or bad CC can be for them.

CC is not a new technology as one might think, but it became a global market trend and one day, all businesses will move to the cloud, as an IT consultant said: *"….it will be the future and someday everything will be on the cloud."* In Egypt, moving to the cloud is termed as a journey to the cloud and even a long journey; this journey will be successfully accomplished in collaboration with all stakeholders. The deputy to the minister of CIT stated that *"…it is a journey to the cloud and it is going to be a long way…..this is just the start and we are going to continue the journey together."* The journey has just started with collective efforts to enable the adoption of CC in Egypt to leverage its economic status, and will continue to overcome inhibiting obstacles.

7. Conclusion

This paper provided an overview on the ongoing journey to the cloud in Egypt. This is achieved by conducting an exploratory case study to understand how CC adoption in Egypt is influenced. The findings from the case study are analyzed by applying concepts of neo-institutional theory (i.e., isomorphic pressures and strategic responses to institutional processes) to identify factors inhibiting the adoption of CC in Egypt, as well as the enabling factors as a set of workarounds to deal with some inhibiting factors. Furthermore, the paper demonstrated the various stages and models of adopting CC in Egypt. The paper provides some facts and lessons from the Egyptian journey to CC.

Table 4: Isomorphic pressures in the Egyptian context

Isomorphic pressures	Contextual descriptions	Sources
Coercive	Vendor lock-in at the level of SaaS service model (i.e., the customer would have to start over all requirements analysis, design, and development in case of changing the provider)	- CSPs
Normative	- Cairo ICT conference (workshops, sessions, and panel discussions) - Training programs offered for university graduates, employees, business owners, and technical professionals - Standards by professional associations and CSPs	- MCIT - Local and international CSPs - Training institutes (i.e., ITI and TIEC) - PCI security standards council and International Organization for Standardization (ISO)
Mimetic	- Global business trends - Showcasing successful implementations of cloud computing models - Consulting advices on how and when cloud computing can be beneficial for businesses	- Competitors - Peer organizations - Consultancy firms

Table 5: Strategic responses to isomorphic pressures

Strategic responses	Tactics	Description	Justification
Acquiescence	- Imitate	Acceptance of advice from consulting firms or professional associations and full implementation of public cloud solutions	To increase flexibility and improve public services of government customers
Compromise	- Bargain	Negotiation with stakeholders (i.e., CSPs, government and business customers)	To reach a practical solution for implementing governmental cloud
	- Pacify	Accommodating multiple isomorphic pressures by implementing hybrid clouds (i.e., implementing private cloud and offering public clouds)	To ensure full control over the infrastructure and gain legitimacy in ICT market by being CSPs
Avoidance	- Conceal	Disguising the intention not to implement cloud computing solutions by proofing concept of them	To demonstrate the feasibility of cloud solutions without intention to implement (i.e., using cloud services as a test environment)
Defiance	- Dismiss	Resistance to implement CC model as it is perceived as a threat to the customers' business	- Political uncertainty: distrust that arbitrary Internet cut by government will not happen again - Limited connectivity as an overall problem in Egypt - Data security concerns resulting from cultural and legal issues - Resistance to change (i.e., rigidity of Egyptian businesses vs. flexibility of international ones, and job threat) - Lack of awareness
Manipulation	- Influence	Implementation of private clouds as a criteria of acceptable practice	To guarantee security of the data and full control of the infrastructure, especially, customers who operate in banking industry

References

[1] Abou El-Seoud, M.S., El-Sofany, H.F., Taj-Eddin, I. a. T.F., Nosseir, A., and El-Khouly, M.M. Implementation of Web-Based Education in Egypt Through Cloud Computing Technologies and Its Effect on Higher Education. *Higher Education Studies 3*, 3 (2013), 62–76.

[2] Avgerou, C. The Link Between ICT and Economic Growth in The Discourse of Development. *Proceedings of the International Federation of Information Processing, IFIP 9.4 and 8.2 Joint Conference on Organizational Information Systems in the Context of Globalization*, (2003), 373–386.

[3] Avgerou, C. Discourses on ICT and Development. *Information Technologies and International Development 6*, 3 (2010), 1–18.

[4] Bhat, J.M. Adoption of Cloud Computing by SMEs in India : A study of The Institutional Factors. *Proceedings of the 19th Americas Conference on Information Systems*, (2013), 1–8.

[5] Bilbao-Osorio, B., Dutta, S., Geiger, T., and Lanvin, B. The Networked Readiness Index 2013 : Benchmarking ICT Uptake and Support for Growth and Jobs in a Hyperconnected World. 2013, 3–33. http://www3.weforum.org/docs/GITR/2013/GITR_Chapter1.1_2013.pdf.

[6] Bose, I., Saha, D., and Huang, M. Sanchari : Moving Up the Value Chain Through Telecommunication Services. *Communications of the Association for Information Systems 30*, 1 (2012).

[7] Cavaye, A.L.M. Case Study Research: A Multifaceted Research Approach for IS. *Information Systems Journal 6*, 3 (1996), 227–242.

[8] Cleverley, M. Emerging Markets: How ICT Advances Might Help Developing Nations. *Communications of the ACM 52*, 9 (2009), 30.

[9] Darke, P., Shanks, G., and Broadbent, M. Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism. *Information Systems Journal 8*, 4 (1998), 273–289.

[10] DiMaggio, P. and Powell, W. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review 48*, 2 (1983), 147–160.

[11] Dowling, J. and Pfeffer, J. Organizational Legitimacy: Social Values and Organizational Behavior. *The Pacific Sociological Review 18*, 1 (1975), 122–136.

[12] Dutta, S., Bilbao-Osorio, B., and Geiger, T. *The Networked Readiness Index 2012: Benchmarking ICT Progress and Impacts for the Next Decade*. 2012.

[13] Dutta, S. and Mia, I. *The Global Information Technology Report 2010–2011*. 2011.

[14] Eisenhardt, K.M. Building Theories from Case Study Research. *The Academy of Management Review 14*, 4 (1989), 532–550.

[15] eMarketing Egypt. *Facebook in Egypt: E-Marketing Insights*. 2013.

[16] Greengard, S. Cloud Computing and Developing Nations. *Communications of the ACM 53*, 5 (2010), 18.

[17] Gregor, S. The Nature of Theory in Information Systems. *MIS Quarterly 30*, 3 (2006), 611–642.

[18] Hana, M.A. E-government Cloud Computing Proposed Model: Egyptian E_Government Cloud Computing. *The International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Ieee (2013), 847–852.

[19] Information Economy Report. *Information Economy Report 2013: The Cloud Economy and Developing Countries*. 2013, i-118. http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.

[20] ITU. *Measuring the Information Society*. 2011, 1-174. http://www.itu.int/ITU-D/ict/publications/idi/material/2011/MIS_2011_without_annex_5.pdf.

[21] ITU. *Measuring Information Society*. 2013, 1-254. http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf.

[22] Iyer, E.K., Krishnan, A., Sareen, G., and Panda, T. Analysis of Dissatisfiers That Inhibit Cloud Computing Adoption Across Multiple Customer Segments. *Proceedings of the European Conference on Information Management & Evaluation*, (2013), 145–152.

[23] Jiao, Y., Wang, Y., Zhang, S., Li, Y., Yang, B., and Yuan, L. A Cloud Approach to Unified Lifecycle Data Management in Architecture, Engineering, Construction and Facilities Management: Integrating BIMs and SNS. *Advanced Engineering Informatics 27*, 2 (2013), 173–188.

[24] Kamal, M. and Anand, V. A Path to Socio-economic Development Using Cloud Computing. *Proceedings of the 2013 46th Hawaii International Conference on System Sciences*, Ieee (2013), 4207–4216.

[25] Kshetri, N. Cloud Computing in Developing Economies. *Computer 43*, 2010, 47–55.

[26] Kshetri, N. Cloud Computing in India. *IT Professional 14*, 2012, 5–8.

[27] Lai, I.K.W., Tam, S.K.T., and Chan, M.F.S. Knowledge Cloud System for Network Collaboration: A Case Study in Medical Service Industry in China. *Expert Systems with Applications 39*, 15 (2012), 12205–12212.

[28] Luoma, E. and Nyberg, T. Four Scenarios for Adoption of Cloud Computing in China. *Proceedings of the European Conference on Information Systems (ECIS 2011)*, (2011).

[29] Marston, S., Li, Z., Bandyopadhyay, S., and Ghalsasi, A. Cloud Computing – The Business Perspective. *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2011)*, (2011), 1–11.

[30] MCIT. *MCIT Yearbook 2013*. 2013, 1-91. http://www.mcit.gov.eg/Upcont/Documents/Yearbook2013_Final.pdf.

[31] MCIT. *A Devoted Candidate for the ITU Council 2014-2018*. 2014, 1-15. http://mcit.gov.eg/Upcont/Documents/ITUBrochure-(2014-2018)-March18.pdf.

[32] Mell, P. and Grance, T. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. 2011, 1–7. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[33] Microsoft. *Bank Improves the Availability of its Products and Services through Cloud Computing*. 2012, 1-2. http://www.microsoft.com/casestudies/Windows-Server/National-Bank-of-Egypt/Bank-Improves-the-Availability-of-its-Products-and-Services-through-Cloud-Computing/710000001377.

[34] Mignerat, M. and Rivard, S. Positioning the Institutional Perspective in Information Systems Research. *Journal of Information Technology 24*, 4 (2009), 369–391.

[35] Nasr, A.A.O. and Galal-edeen, G.H. Proposed Development Model of e-Government to Appropriate Cloud Computing. *International Journal of Reviews in Computing 9*, 7 (2012), 1–7.

[36] Oliver, C. Strategic Responses to Institutional Processes. *The Academy of Management Review 16*, 1 (1991), 145–179.

[37] Orlikowski, B.W.J. and Barley, S.R. Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other? *MIS Quarterly 25*, 2 (2001), 145–165.

[38] Orlikowski, W.J. and Baroudi, J.J. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research 2*, 1 (1991), 1–28.

[39] Osman, F., Smith, B., Sherin, O., et al. Egypt Revolution. *Blue Kaizen*, 2011, 4–9. http://www.bluekaizen.org/securitykaizen_mag/issue2/Security_Kaizen_2.pdf.

[40] Report Arab Social Media. Twitter in The Arab Region. 2013. http://www.arabsocialmediareport.com/Twitter/LineChart.aspx?&PriMenuID=18&CatID=25&mnu=Cat.

[41] Salem, F. and Mourtada, R. *Social Media in the Arab World : Influencing Societal and Cultural Change ?* 2012, 1-29. http://www.dimed.gouv.fr/sites/dimed.gouv.fr/files/asmr_-_social_media_in_the_arbian_world-influencing_societal_and_cultural_change_-_juillet_2012.pdf.

[42] Scott, W.R. Unpacking Institutional Arguments. In W.W. Powell and P.J. DiMaggio, eds., *The new institutionalism in organizational analysis*. University of Chicago Press, Chicago, 1991, 143 – 163.

[43] Scott, W.R. *Institutions and Organizations*. Sage, 2001.

[44] Su, N., Akkiraju, R., Nayak, N., and Goodwin, R. Shared Services Transformation : Conceptualization and Valuation from the Perspective of Real Options. *Decision Sciences 40*, 3 (2009), 381–402.

[45] Suchman, M.C. Managing Legitimacy: Strategic and Institutional Approaches. *The Academy of Management Review 20*, 3 (1995), 571–610.

[46] Sultan, N. Cloud Computing: A Democratizing Force? *International Journal of Information Management 33*, 5 (2013), 810–815.

[47] Tang, X., Chiang, C.-Y., Liu, Z., and Lin, J. Application Service Provider (ASP) in China: An Empirical Study of System and Service Satisfaction. *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS 2011)*, (2011), 1–10.

[48] Truong, H., Pham, T.-V., Thoai, N., and Dustdar, S. Cloud Computing for Education and Research in Developing Countries. *Cloud Computing for Teaching and Learning: Strategies for Design and Implementation*. 2012, 78–94.

[49] Tsao, H.J., Parikh, S., Ghosh, A.S., et al. Streamlining Grain Supply Chains of India: Cloud Computing and Distributed Hubbing for Wholesale-retail Logistics. *Proceedings of the IEEE International Conference on Service Operations and Logistics and Informatics (SOLI)*, (2010).

[50] Venters, W. and Whitley, E. a. A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology 27*, 3 (2012), 179–197.

[51] Wahid, F. and Sein, M.K. Steering Institutionalization through Institutional Work: The Case of an eProcurement System in Indonesian Local Government. *Proceedings of the 47th Hawaii International Conference on System Sciences (HICSS 2014)*, (2014), 4264 – 4274.

[52] Walsham, G., Robey, D., and Sahay, S. Special Issue on Information Systems in Developing Countries. *MIS Quarterly 31*, 2 (2007), 317–326.

[53] Walsham, G. Interpretive Case Studies in IS Research : Nature and Method. *European Journal of Information Systems 4*, (1995), 74–81.

[54] Yin, R.K. Designing Case Studies: Identifying Your Case (s) and Establishing The Logic of Your Case Study. In *Case Study Research: Design and Methods*. SAGE Publications, Incorporated, London, 2009, 25–66.

STRATEGIES FOR CLOUD COMPUTING ADOPTION: INSIGHTS FROM THE NORWEGIAN PUBLIC SECTOR

Rania Fahim El-Gazzar, Department of Information Systems, University of Agder, Kristiansand, Norway rania.f.el-gazzar@uia.no

Fathul Wahid, Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia, and Department of Information Systems, University of Agder, Kristiansand, Norway
fathul.wahid@uii.ac.id

Abstract

This study aims to understand the adoption of cloud computing in the Norwegian public sector. Although considered a well-informed adopter of cloud computing, Norway's adoption rate in the public sector is still low. Using a case study method guided by institutional theory, we defined field level changes, which created various isomorphic pressures: coercive, normative, and mimetic. The pressures have been responded differently by government agencies, which manifested in their strategy for adopting cloud computing, from adopting a public cloud to developing their own private cloud infrastructure. The study went further by identifying factors that either hinder or foster the adoption. Reasons behind non-adoption related to unsolved complexity, organizational conflicts, and specific business needs, but not risks of the cloud computing model itself. Furthermore, the study found that a certain strategic response could trigger a new pressure, which might be more aggressive. It revealed that previous unlikely incidents reported in the media had influenced the Norwegian public organization's adoption strategy.

Keywords: cloud computing, public sector, institutional theory, isomorphic pressure, strategic response, developed country, Norway.

1 INTRODUCTION

The prevailing global market trends toward Cloud Computing (CC) and the enticing benefits it offers are inevitable for businesses (Marston et al. 2011; CA Technologies 2013). CC has shifted responsibilities, roles, and the way organizations run their businesses and manage their IT resources (Ragowsky et al. 2014; Schneider & Sunyaev 2014). CC brings desired agility, scalability, economies of scale, and strategic values to organizations; yet, it poses concerns and uncertainties (Venters & Whitley 2012; Schneider & Sunyaev 2014; Garrison et al. 2012; Malladi & Krishnan 2012). Concerns related to the adoption of CC range from technical and organizational to environmental (i.e., both business and legal) (Marston et al. 2011; Morgan & Conboy 2013; Owens 2010). Public organizations perceive CC as a steering wheel that drives innovation in delivering better public services (EN 2012; Frelle-Petersen et al. 2012). However, public organizations also perceive the risks associated with adopting cloud services, which mainly relate to technical, security, and legal issues (Paquette et al. 2010; Seddon & Currie 2013). To the best of our knowledge, limited research efforts focused on legal and business issues still exist (Yang & Tate 2012).

Despite previous research focused on identifying and addressing those risks, CC adoption rates in the public sector increase more slowly than in the private sector (Hawkins 2013). Likewise, although Norway is reported to be a promising market for CC, both in the private and public sectors (Haeberlen et al. 2013), the adoption rates in the Norwegian public sector (33%) are lower than the Norwegian private sector (38%) (Kristiansen 2011). The Norwegian public sector (i.e., municipalities, public organizations, and public authorities) began considering CC in their strategy (Ministry of Local

Government and Modernization 2013; Devoteam daVinci 2011). Accordingly, CC providers began investing in a more reliable infrastructure such as the capacity of data networks (Telenor 2013).

However, Norwegian public organizations' experience with CC was confronted with several challenges, and their adoption did not always go smoothly (O'Donoghue 2012; Veum & Thoreid 2012; Jørgenrud 2011). Hence, it is important to understand their motivation and the strategy behind their adoption. Against this backdrop, this study sought to answer the following questions: *How is CC adoption in the Norwegian public sector influenced by the surrounding institutional environment? Why did they respond differently to these influences?*

In seeking these answers, we conducted an interpretive case study in the context of the Norwegian public sector. We used neo-institutional theory to guide our data analysis. This paper begins with the background of CC definition and CC research stream in the public sector in Section 2, followed by the background of borrowed concepts from the neo-institutional theory. Section 3 presents a description of the contextual setting and data collection for the case study method used in Section 4. Section 5 shows the findings framed within the neo-institutional theory concepts. The findings discussed in Section 6 by highlighting the insights gained from the case study, conclusions, and limitations.

2 CLOUD COMPUTING IN THE PUBLIC SECTOR

There is considerable interest in CC from public sector organizations; for them, CC "represents a fundamentally different way for government to architect computing resources, allowing governments to leverage powerful IT infrastructures in a fraction of the time it takes to provision, develop, and deploy similar assets in-house" (Shin 2013, p.194). With CC services, public organizations can reduce IT capital expenditures through pay-per-use subscription and improve their services to the public as well as overcome difficult financial crises (Haeberlen et al. 2013; Sultan 2010). However, public organizations are still lag behind private organizations in adopting CC services (Hawkins 2013; Baldwin 2012); this slow adoption has three reasons.

Firstly, the meaning of CC is not clear despite the literature contributed to defining the CC model and differentiating it from previous IT models (i.e., clusters and grids (Buyya et al. 2009)) and business models (i.e., IT outsourcing (Schneider & Sunyaev 2014)). Hence, CC definition states, "computing services are delivered over the Internet, on demand, from a remote location, rather than residing on one's own desktop, laptop, mobile device, or even on an organization's servers. For an organization, this would mean that, for a set or variable, usage-based fee—or even possibly for free—it would contract with a provider to deliver applications, computing power, and storage via the web" (Wyld 2009, p.6). CC services are offered as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) (Mell & Grance 2011). These services are deployed as public, private, or hybrid, based on the criticality of the data and applications (Mell & Grance 2011).

Secondly, data security risks regarding citizens' records are further serious concerns that require adequate risk management approaches (Paquette et al. 2010) to assure that data confidentiality, integrity, and availability can address a wide range of security risks (Zissis & Lekkas 2011) to promote better experiences using CC services in the public sector (Shin 2013). In this regard, the literature contributed to introducing models for guiding the selection of CC services based on technical (i.e., security and performance) and economic (i.e., cost) criteria (Broberg et al. 2009; Garg et al. 2013).

Thirdly, laws and regulations related to data protection and privacy in the cloud, which constrain the exchange of public data through the cloud in highly regulated sectors, such as healthcare, are not mature or ready to regulate the CC industry (Schneider & Sunyaev 2014). These legal struggles pose enormous challenges to policy-makers regarding how to sustain the adoption of CC in the public sector and clarify the responsibilities of both public organizations and cloud providers (Seddon & Currie 2013; Wyld 2009). Hence, both public organizations and cloud providers should cooperate on complying with strict regulations "to avoid penalties for non-compliance and possible reputational damage if exposed by the media" (Seddon & Currie 2013, p.230). Thus, governments have to address a set of challenges to facilitate using a variety of CC services in public organizations (Wyld 2009).

The literature covered areas related to addressing security issues, providing adoption guidelines, and explaining legal struggles in the public sector (Shin 2013; Paquette et al. 2010; Zhao et al. 2013; Seddon & Currie 2013). However, the literature did not explain why public organizations follow different adoption strategies toward CC services. Hence, we aimed at exploring the institutional influences that affect the adoption of CC services in the Norwegian public sector and the reasons for different strategic responses to influences exerted by Norwegian public organizations.

3 THEORETICAL UNDERPINNINGS

Neo-institutional theory has been used to study Information Systems (IS)/IT-related phenomena in terms of adoption and use of IS/IT innovations in organizations in general (Currie 2009; Mignerat & Rivard 2009; Weerakkody et al. 2009) and in the public sector in particular (Wiredu 2010; Currie & Guah 2007). CC is an innovative IS/IT outsourcing model; its idea of 'shared services' enables enhancing organizations' architectural agility and improving organizational learning and innovation (Su et al. 2009). Neo-institutional theory is a better lens to understand, in the context of IS/IT outsourcing, "how social choices are shaped, mediated, and channelled by institutional arrangements ...and how actors and their interests are institutionally constructed" (Currie 2004, p.238).

Organizations are required to conform to a set of rules and requirements at the organizational field level to legitimize themselves (Wooten & Hoffman 2008). The organizational field is defined as "a community of organizations that partakes of a common meaning system and whose participants interact more frequently and fatefully with one another than with actors outside the field" (Scott 2001, p.84). This may include regulatory bodies, business partners (i.e., customers and suppliers), peer organizations, competitors, and professional and trade associations.

Orlikowski and Barley (2001) argued that neo-institutional theory is helpful for understanding 'how technologies are embedded in complex interdependent social, economic, and political networks, and how they are consequently shaped by broader institutional influences' (p.154). These institutional influences enable or constrain organizations' behaviour (Orlikowski & Barley 2001), and they are imposed by the community of organizations that create changes at the organizational field level in which the adopting organization operates. These isomorphic pressures are (DiMaggio & Powell 1983): coercive, normative, and mimetic (see Table 1).

Isomorphic pressure	**Description**
Coercive	Imposed by the legal environment and can be either formal (i.e., laws and standards) or informal (i.e., cultural)
Normative	Imposed by professional associations, universities, and training institutions to produce guidelines for professional behaviour or individuals with similar orientation
Mimetic	Imposed by environment uncertainty and goal ambiguity so that organizations model themselves on other successful organizations in their field

Table 1. Isomorphic pressures

Organizations can respond differently to the three isomorphic pressures through five strategic responses to legitimize themselves within their organizational field (Oliver 1991). These strategic responses are (see Table 2): (1) acquiescence: when the organization conforms to institutional norms through imitate, habit, or comply tactics; (2) compromise: when the organization accommodates multiple institutional stakeholders through balance, pacify, or bargain tactics; (3) avoidance: when the organization precludes the need for conformity to institutional norms through conceal, buffer, or escape tactics; (4) defiance: when the organization resists the institutional norms through dismiss, challenge, or attack tactics; and (5) manipulation: when the organization actively exerts power over the sources of the pressure by applying co-opt, influence, or control tactics on institutional constituents.

Strategies	Tactics	Examples
Acquiescence	Habit	Following invisible, taken-for-granted norms
	Imitate	Mimicking institutional models
	Comply	Obeying rules and accepting norms
Compromise	Balance	Balancing the expectations of multiple constituents
	Pacify	Placating and accommodating institutional elements
	Bargain	Negotiating with institutional stakeholders
Avoidance	Conceal	Disguising nonconformity
	Buffer	Loosening institutional attachments
	Escape	Changing goals, activities, or domains
Defiance	Dismiss	Ignoring explicit norms and values
	Challenge	Contesting rules and requirements
	Attack	Assaulting the sources of institutional pressure
Manipulation	Co-opt	Importing influential constituents
	Influence	Shaping values and criteria
	Control	Dominating institutional constituents and processes

Table 2. Strategic responses and tactics (Oliver 1991)

4 RESEARCH SETTING AND METHOD

4.1 The setting

According to Global Information Technology (GIT) reports from three consecutive years 2012, 2013, and 2014, Norway ranked among the top 10 advanced economies being the 7th, 5th, and 5th respectively (Schwab & Greenhill 2012; Bilbao-Osorio et al. 2013; Schwab & Eide 2014). Furthermore, GIT reports recorded Norway's substantial positions in those three years as being a ready society for Information and Communication Technology (ICT) as measured by the Networked Readiness Index (NRI) in terms of environment friendliness for ICT, readiness to use ICT, actual usage of ICT by all stakeholders, and the impact of ICT on the economy and society. As demonstrated in Table 3, Norway recorded greater progress in 2014 than 2012 and 2013 in most of the readiness indices; however, the economic and social impact of ICT in Norway is not yet stable. In terms of readiness for cloud services, Norway is among the cloud prepared countries, according to a recent report by Cisco (Cisco 2013). Norway meets the minimum requirements for advanced cloud services in terms of key cloud infrastructure indicators are in place (i.e., hardware, network security, and Internet speed) (Information Economy Report 2013).

Readiness index	Rankings over years		
	2012	2013	2014
Environment friendliness for ICT (i.e., political and regulatory, business and innovation)	10	9	7
Readiness for making good use of ICT (i.e., ICT infrastructure and accessibility of digital content, cost of accessing ICT, and basic educational skills for effective use of ICT)	6	6	4
Actual usage of ICT (i.e., individuals, businesses, and government)	6	7	6
Impact of ICT in gaining economic and social competitiveness	13	11	12

Table 3. The rankings of Norway across ICT readiness indices of the NRI. Sources: Schwab and Eide (2014), Schwab and Greenhill (2012), and Bilbao-Osorio et al. (2013)

4.2 The method

To explore how the adoption of CC in Norway is influenced and why organizations respond differently to institutional influences, the researchers conducted an exploratory case study to address the how and why questions (Yin 2009). Case study strategy is useful in understanding the dynamics of the context of the phenomenon under investigation (Darke et al. 1998; Yin 2009) and the human/technology interaction in the natural social setting (Orlikowski & Baroudi 1991). Two main sources provided the basis for this paper's data: (1) 9 semi-structured interviews conducted through various communication modes; and (2) document analysis (i.e., research articles, reports, and official documents generated by Datatilsynet, the Norwegian government authority, and news articles). Interviewees represented various stakeholders (i.e., cloud service providers, consultancy, and customer organizations from the public sector). We chose the informants purposefully based on their knowledge about and/or experience with CC (Patton 1990; Palinkas et al. 2013) as demonstrated in their profiles, shown below in Table 4.

Code	Position	Institution	Interview mode	Interview duration
Customer 1	CIO	Municipality	Phone	25 min
Customer 2	Enterprise architect	Government regional authority	Microsoft Lync	44 min
Customer 3	IT advisor	Municipality	Face-to-face	44 min
Customer 4	CIO	Municipality	Phone	23 min
Customer 5	Assistant director	Government agency	Face-to-face	42 min
Customer 6	Technical project manager	Government agency		
Consultant 1	Senior security consultant	Public IT consulting company	Face-to-face	89 min
Consultant 2	Cloud advisor	Public IT consulting company	Skype	32 min
Provider 1	Product manager	Private IT services company	Face-to-face	56 min

Table 4. Informants' profiles

5 FINDINGS AND ANALYSIS

5.1 Changes at the organizational field

This study aimed to explain the institutional influences that facilitate and/or constrain the adoption of CC in the Norwegian public sector, how public organizations strategically balance their need to move their IT environment to the cloud, and the requirements from both the legal and business environments. The defined organizational field for this study included all stakeholders (i.e., Ministry of Government Administration, Norwegian Data Protection Authority [Datatilsynet], professional consultancy, customer organizations from the public sector, and cloud providers). The findings from this study were framed within the isomorphic pressures (i.e., coercive, normative, and mimetic) to identify factors that influence the adoption of CC in Norway, followed by the identification of various adoption strategies by public organizations framed within the strategic responses (i.e., acquiescence, compromise, avoidance, defiance, and manipulation) with given rationales.

5.2 Isomorphic pressures

5.2.1 Coercive

After experiences with Narvik and Moss municipalities (Veum & Nymoen 2012; Veum & Thoreid 2012; O'Donoghue 2012), opinions about CC changed. These two municipalities used public SaaS cloud models; Narvik used Google Apps (i.e., e-mail and file sharing) and Moss used Microsoft Office 365 (Datatilsynet 2012). Moving to the public cloud was an expensive experience for Narvik, and an alert for Datatilsynet to safeguard the use of public clouds in municipalities. Consultant2 stated,

> *"two municipalities in Norway that moved to the public cloud last year; one to Microsoft and one to Google and they spent millions of kroners on lawyers in order to sort out the laws and regulations that were affected by moving to the public cloud…but of course they are early adopters so they had to use some money on it, and they got some good feedback and guidelines on how to approach the cloud, which was good after all!".*

Datatilsynet banned the use of Google Apps in Narvik after finding that Google's data processor agreement did not fulfil information security requirements, according to the Norwegian law, regarding the location of the data, and Narvik did not conduct proper risk assessments (Veum & Thoreid 2012; Thon & Vetland 2012; Gould 2012). Datatilsynet had a concern about the U.S. Patriot Act and required Narvik to conduct risk assessment to get more information about data location, data segregation, and access controls (Gould 2012).

Nine months later, Datatilsynet decided to let Narvik municipality continue to use Google Apps (Essers 2012), but conditionally upon certain guidelines (Datatilsynet 2012). Moss municipality requested a review and guidelines from Datatilsynet for using Microsoft Office 365 (Veum & Nymoen 2012). These guidelines are explained by Consultant1,

> *"When they were finished with going through these cases [Narvik and Moss], we discovered three things that were very important: (1) it is required by the Norwegian law, risk analyses [before moving to the cloud]; (2) have an agreement [called databehandleravtale that is available on Datatilsynet's home pages] with the cloud service provider with specific needs according to the Norwegian law. So you cannot use the agreement directly from Microsoft…and Microsoft knows about it…; (3) implement regular security audits of Microsoft if you choose Microsoft, and of Google if you choose Google. So Moss and Narvik, they now get information about security audits on Microsoft and Google".*

Furthermore, Consultant1 stressed that municipalities cannot use CC services without these three guidelines and that the responsibility is on the municipalities to ensure that the cloud provider processes the personal data according to the Norwegian data privacy regulations. If something went wrong with the data, the first entity will be questioned is the customer organization or the municipality. Therefore, for municipalities, CC is neither fully prohibited nor fully allowed, but they must be cautious as Provider1 stated,

> *"Datatilsynet, they say it is not by itself illegal to store data on a server outside Norway. But, you have to consider each case and make sure it is not sensitive data. So they don't give a green flag for all types of scenarios".*

In addition to the guidelines offered to municipalities regarding the use of CC services, there were lessons learnt by the Norwegian legal system to upgrade and address the challenges brought by using CC services. In this regard, Consultant1 contended,

> *"These two cases [Narvik and Moss] are what we need to look at to see and compare with for future cases because every detail of the law is not regulated because cloud services systems are new things and they are a lot between different countries [laws] and there are so many new things for the Norwegian law and the court systems to go through, so they mainly take a few cases and they build next cases on laws".*

5.2.2 Normative

CC adoption in Norway is influenced by learning processes of exchanging knowledge about professional guidelines to deploy CC services. Norway established its own strategic initiative called 'Digital Agenda for Norway', putting CC among other digital goals; cloud services offer flexible and low-cost solutions for public and private sectors, as well as create jobs and businesses in Norway rapidly (Ministry of Local Government and Modernization 2013; Etro 2009). Accordingly, the Ministry of Government Administration, Reform, and Church Affairs encourages public agencies to procure cloud services (Ministry of Local Government and Modernization 2013).

CC adoption remains slow in the Norwegian public sector due to lack of experience and knowledge about CC among Norwegian organizations. This led the 10 largest Norwegian municipalities to form a

cooperation forum called K10[1] in collaboration with the Norwegian Association of Local and Regional Authorities (KS) to speed up the adoption of cloud services in Norway (Hustad & Olsen 2012; Devoteam daVinci 2011). The purpose of the K10 forum is to exchange knowledge about CC, establish common municipal ICT architecture, and influence ICT policies of public sector agencies regarding procurement, standards, and cloud service models (Hustad & Olsen 2012; Devoteam daVinci 2011). Furthermore, Hustad and Olsen (2012) argued that the adoption of CC services in Norway will be driven strategically by business value rather than economically by low-cost decisions.

5.2.3 Mimetic

One study claimed that demonstrating successful stories of pioneer Norwegian organizations adopting CC solutions and growing significantly is a key motive to adopting CC in Norway (Hustad & Olsen 2012). Cloud providers can show their specialities in various CC service models (e.g., SaaS, PaaS, IaaS), references, and successful stories on their websites (Microsoft 2013; Xledger 2014) to gain credibility and convince potential customers to use their cloud services, especially when their reference customers are from the public sector or the field of heavy industries. Pure Norwegian cloud providers, such as JottaCloud and Evry, also demonstrate their compliance with the Norwegian legislation and privacy regulations, and their physical storage of data in Norway (Andino 2013; Evry 2014). This conveys their independence from the Patriot Act and makes it a competitive advantage for them to grow in the cloud market. Thus, customer organizations do not have to worry about the location of the data or if the foreign international cloud provider is complying with the Safe Harbor agreement. Regarding local providers, Consultant2 said that he understands the customer organizations' fear of dealing with foreign international cloud providers. He asserted,

> *"I think that goes more back to the rules and regulations and where data are physically stored. I have seen that Norwegian cloud providers, especially backup services and those kinds of things have got a lot of attention lately because then you don't store data anywhere near the NSA".*

Thus, local cloud providers represent a safe option for some customer organizations to avoid inspection by Datatilsynet as happened with Narvik municipality, and ensure adherence to the Norwegian regulations.

5.3 Strategic responses

5.3.1 Acquiescence

At first, Narvik municipality used Google Apps without a thorough risk analysis and without a clear statement about the data location (Gould 2012); this implied that the municipality used the imitation tactic to unconsciously mimic the model of Google's public CC services for the following reasons (Jørgenrud 2011): (1) efficiency: reducing maintenance costs to focus more on strategic issues, desiring mobile solutions, and seeking new functionality after their previous software environment, that is IBM Lotus Notes, became outdated and they lacked the right skills to maintain it; and (2) limited alternatives: Narvik sent requests to IBM, Microsoft, and Google, but only Google responded to their request. Therefore, Narvik chose to enter into an agreement with Google Apps.

After banning Narvik from using Google Apps, the municipality used the comply tactic to gain legitimacy by adhering to Datatilsynet's restrictions through changing their contract with Google and obtaining additional assurances and information about location of the data from Google (Gould 2012). Moss municipality used the comply tactic by following consciously the guidelines they requested from Datatilsynet before beginning use of Microsoft Office 365 cloud to gain legitimacy (Veum & Nymoen 2012; Datatilsynet 2012). Furthermore, Moss chose Microsoft Office 365 public cloud for the sake of efficiency: improving work quality of their public employees, seeking flexibility in administering users, and avoiding the hassle of IT maintenance operations (Moss Kommune 2013).

[1] The ten largest municipalities in Norway (i.e., Oslo, Bergen, Trondheim, Stavanger, Kristiansand, Drammen, Fredrikstad, Tromso, Sandnes, and Bærum) created K10 in 2010.

Another municipality used Microsoft Office 365; they used the comply tactic to gain legitimacy by following the legal requirements set by Datatilsynet, and they hired external companies to ensure this compliance. In this regard, Customer1 stated,

> *"We have some services in the cloud, we have Office 365. But, all employees store data on-premise. We have our own guidelines for risk evaluation [set by Datatilsynet for municipalities], but we have an external company that handles this for us today, but the most important thing is that we understand different risks like, for example, loss of data. And, the most important is how the data are stored".*

Another municipality used Microsoft cloud services at length and used the comply tactic, through which they unconsciously used the data processing agreement provided by Datatilsynet to gain legitimacy. In this regard, Customer4 asserted,

> *"My organization uses quite a few cloud services, especially, from Microsoft [Office 365] platform, and so we have been adopting cloud services for quite long time. Norwegian government organizations need, in Norwegian term, Databehandleravtale [data processing agreements]. Without them, we cannot use cloud services. I feel, at least, that we have to accept what we have got!"*

Furthermore, they used CC services for efficiency purposes: automation of IT resources and serving the public efficiently. Customer4 said,

> *"We need to find a way [to use] public clouds to provide the service to the public in a new and more efficient way with focus on automation and to a larger extent than what we do on-premise".*

5.3.2 Compromise

Another government regional authority currently considering use of CC services has two trajectories planned toward adopting CC. In the first trajectory, they used the bargain tactic to negotiate sourcing strategies with sourcing partners to deliver PaaS and IaaS service models to their associated enterprise units. Their reason for doing so is efficiency: to simplify and regionalize their IT architecture. They are now describing the specifications of the future IT architecture to transition from a more distributed one to a more simplified and consolidated regionalized one. Customer2 explained,

> *"We haven't moved to utilize cloud services yet. At the moment, we have a shared service provider [SSP] and we are in the phase of transitioning SSP to become more focused on the application services side, and the business process side…..we have a program at the moment called infrastructure modernization, so a part of its mandate is to look at sourcing strategies and sourcing partners to be able to deliver platform as a service and infrastructure as a service".*

Customer 2 asserted that laws and regulations constrain their choice of CC sourcing partners, and they need to follow those regulations to gain legitimacy. The second trajectory towards adopting CC in this organization follows in the next sub-section on avoidance strategy.

5.3.3 Avoidance

In the abovementioned government regional authority, they did not transition to and use CC services; nonetheless; they used the conceal tactic. They aimed at efficiency by testing Microsoft Azure solution to evaluate its functionality for building mobile solutions and regional electronic public record solutions. Additionally, they are testing the CC solution to avoid facing complexity with the regional electronic public record because of its connection to many existing systems. In this regard, Customer2 stated,

> *"We have at least two evaluation initiatives, and proof-of-concept initiatives are ongoing. One of them is concerned with testing or proofing concept of the environment for mobility solutions where some of the storage of the data is done in the cloud…[where] some of the documentation which is generated by personnel…using iPads and the service we are using is Microsoft Azure in that environment, and also the other initiative is more in early stages; we are looking at how*

can we utilize the cloud in the context of establishing a regional electronic [public] record solution which is centralized, consolidated, and standardized [across associated enterprise units]. And, that is too complicated because the electronic [public] record is integrated with many systems and that is why integration can pose a concern".

5.3.4 Defiance

Another municipality did not initiate the adoption strategy and used the dismiss tactic by ignoring the idea of adopting CC services that are offered and discussed at a small conference, which was held to discuss opportunities in relation to the initiative of common municipal ICT architecture. The reasons for not reaching the proper strategy for using cloud services in this municipality was threefold: (1) loss of control: data sensitivity concern regarding data location; (2) conflicts: with small municipalities joining a big municipality, each has different interests and knowledge about the use of IT; and (3) bureaucracy: the multi-levelled structure of each municipality makes it slow to reach an agreement on any proposed strategy and the gains are not yet clear for them. Customer3 explained, when he was asked if his municipality is using cloud services or planning to do so,

"We haven't a proper process around that yet. We have discussed, but we haven't made any proper strategy around the cloud yet, mostly because of the data sensitivity. Where the data are stored…. If the data are stored in the USA, then we don't have the confidentiality. In our municipality, the main issue is to have a wider cooperation with all [small] municipalities to gather the main components in one place. When a decision matter or the IT department works on a proposal for a strategy, then it must be delivered to the administrative and then the executive, and then it is sent upward to the politicians to be agreed or to be decided whether to do that or not. Those small municipalities have also the same structure and they have different interests, goals, and knowledge about IT and use of IT systems. So our job here is quite a challenge….Two years ago, I put up a small conference for all municipalities to discuss about CC and the vendors were invited two or three of them. We had a full day of discussion and presentations and none of the municipalities decided anything".

Another reason for defiance is goal ambiguity; they are not sure about the exact benefit from CC services. When asked about whether the municipalities decided to make another meeting afterwards or not, Customer3 answered,

"No, because it is not clear what are the gains because it requires a lot and there is this issue of confidentiality. I have a kind of difficulty to give you a clear enough answer because I suppose we are still unclear ourselves".

5.3.5 Manipulation

A Norwegian government agency used the influence tactic by choosing to implement a private PaaS environment to meet the specific nature of their applications that they develop and deploy to serve the public. They decided to implement their own development and testing environment for the following reasons: (1) lack of reference: current PaaS implementations are immature and not widely used in Norway; (2) independence: to gain full control over the testing environment and eliminate the dependency on external suppliers; and (3) image preservation: thorough testing of their type-specific applications is important for them to avoid headlines of newspapers and preserve their reputation. Customer6 explained that strategy,

"We are implementing now both infrastructure as a service layer and on top of that PaaS….Because we have looked at some commodity implementations of PaaS, no real resources with experiences locally in Norway at least. The current PaaS implementations, they are very App-specific. Ok I can deploy one App, but I have 50 [Apps]. That is not going to help that much, so we actually need either to script or automate against the [current] PaaS implementation".

Customer5 highlighted the importance of having internal competence rather than depending on external suppliers and the matter of reputation. She said,

> *"It is not what we want. We get more restrictions. So, we need to make our own PaaS. To have people know what they are talking about, that is always a good solution. To be very dependent on external suppliers….it is really hard…So, you need to have the competence internally. The rules change every year in the [domain we operate in], so it is not a stable system. So, we have a focus on not facing the front page of the newspapers and not making any mistakes. Testing is very important, because we have an issue with reputation".*

In the same line, Customer6 agreed on the matter of reputation. He asserted,

> *"If there is a bug in the system, the receipt may be garbled. And, when we have sent it, it is too late to fix the system. It goes externally and in the worst case on the front page of the newspapers. So, we can't risk it. So, we need to test very thoroughly. That is an important goal of cloud strategy or automation strategy".*

6 DISCUSSION AND CONCLUSIONS

By revisiting the two research questions from the onset, we discuss the corresponding answers, which are framed using concepts from the neo-institutional theory (i.e., isomorphic pressures and strategic responses to institutional processes). This paper presented a case study to explore the isomorphic pressures imposed on Norwegian public organizations by the constellation of various external actors (See Table 5). The adopting organizations interpreted these pressures differently, as mirrored in various chosen strategies to adopt CC services (See Table 6). The chosen strategic responses ranged from willingness to resistance against conformity to pressures. Furthermore, the paper explicated reasons behind each strategic response chosen. Efficiency stood out as a predominant reason among acquiescence, compromise, and avoidance strategies; this indicates rational choice. However, aside from the imitation tactic, this rationality is balanced with irrationality in the acquiescence and compromise strategies by seeking legitimacy.

Pressure type	Description	Source
Coercive	- Banning the use of CC services in Narvik municipality based on legal assessment - Introducing guidelines for using CC services in municipalities (i.e., conducting risk assessment, having a data processing agreement with the cloud provider according to Norwegian law, implementing regular security audits)	- Datatilsynet
Normative	- Encouraging Norwegian public agencies to procure cloud services - Developing specifications for procuring CC services - Exchanging knowledge and establishing common Norwegian municipal ICT architecture with a focus on appropriate sourcing policies (i.e., procurement, standards, cloud SaaS, PaaS, IaaS)	- Ministry of Government Administration, Reform and Church Affairs - Ten large Norwegian municipalities with the Norwegian Association of Local and Regional Authorities
Mimetic	- Offering Various CC service models (i.e., SaaS, PaaS, IaaS) - Demonstrating successful stories online of pioneer organizations adopting CC services	- Cloud providers - Peer organizations
	- Demonstrating compliance with the Norwegian legislation and privacy regulations	- Pure Norwegian cloud providers

Table 5. Isomorphic pressures on Norwegian public organization

Adoption strategy	**Tactic**	**Definition**	**Empirical evidence**	**Reasons**
Acquiescence	Imitate	Either conscious or unconscious mimicry of institutional models	- When Narvik used Google Apps unconsciously without doing proper risk assessment and having a clear statement in the agreement about the location of the data	- Efficiency - Limited resources
	Comply	A conscious obedience to or incorporation of values, norms, or institutional requirements	- After being banned, Narvik changed their contract with Google to get more assurances so that Datatisynet allowed them to continue using Google Apps	- Efficiency - Legitimacy
			- Moss followed Datatilsynet's guidelines before using Microsoft Office 365	- Efficiency - Legitimacy
			- Another municipality hired an external company to perform risk evaluation, as set by Datatilsynet, for using Microsoft Office 365	- Legitimacy
			- Another municipality used the data processing agreement by Datatilsynet to use a few cloud services from Microsoft	- Efficiency - Legitimacy
Compromise	Bargain	The effort of the organization to exact some concessions from an external constituent in its demands or expectations	- In a Norwegian public authority, negotiating sourcing strategies to deliver IaaS and PaaS services to associated enterprise units	- Efficiency - Legitimacy
Avoidance	Conceal	Disguising nonconformity behind a facade of acquiescence	- In a Norwegian public authority, two initiatives for testing cloud solutions to evaluate their functionality: - Mobility solutions - Establish a regional electronic public record solution	- Efficiency - Complexity
Defiance	Dismiss	Ignoring institutional rules and values, when the external institutional rules are perceived to be low or when internal objectives conflict with institutional values or requirements	- Ignoring the idea of adopting cloud services despite a municipality held a conference to discuss opportunities	- Loss of control - Conflicts - Bureaucracy - Goals ambiguity
Manipulation	Influence	Shaping values and criteria of acceptable practices or performance	- A public administration authority chose to implement a private PaaS to meet the specific nature of their applications that they develop and deploy to serve the public	- Lack of references - Independence - Image preservation

Table 6. CC adoption strategies and tactics used by Norwegian public organizations

As seen in Table 5, the legal coercive pressure had a dominant influence on the adoption of cloud computing in the Norwegian public sector. The findings from this study indicated the direct effect of the coercive pressure exerted on the previous case of Narvik as public organizations became cautious regarding their strategies to adopt CC services. This manifested in the acquiescence strategy by using the standard agreement provided by Datatilsynet to procure public CC services along with conducting a thorough risk assessment. The compromise strategy resulted from interpreting coercive pressure and mimetic pressure. It enfolds bargaining between regulations and cloud providers who can meet those regulations to attain legitimacy.

Complexity appeared to be one of the key reasons for the avoidance strategy of full adoption of CC services offered by various cloud providers through the mimetic pressure. This manifested in proofing concept of CC solutions to avoid complexity issues that may arise from the interdependency of many

system modules on public records. Mimetic pressures manifest in looking at reference peer organizations that are pioneers in the field, various service models offered by major cloud providers, and using pure Norwegian cloud providers because they demonstrate their adherence to Norwegian legislation. The mimetic pressure is responded by the influence tactic in the manipulation strategy. Despite the wide variety of CC services offered by cloud providers, they may not be widely used within a certain region or country. This happened with the public organization that chose the manipulation strategy; they decided to build their own cloud environment. Having internal competence allows them cope with their rapidly changing business rules and become less dependent on external providers. Apparently, the indirect effect of Narvik's case spreading in the news headlines—is yet another reason for manipulation strategy.

The normative pressure aimed at exchanging knowledge and developing specifications for procuring CC services by public agencies. Although it is dismissed by some municipalities in a defiance strategy, the fear of losing control over data secrecy was a reason. However, the findings indicate that the dismissal was mainly caused by the bureaucracy, conflict of interests, and goal ambiguity. Hence, the defiance had no direct relation to the risks of the CC model per se.

According to Oliver (1991), the responses are triggered towards the isomorphic pressures as one-way interaction. However, the findings from this study showed that an organization's response to some pressures could trigger further pressures on it. This happened with Narvik when it imitated Google's Apps services without risk assessment. It triggered a new coercive pressure on it from Datatilsynet.

The insights offered by this study may be further compared with CC adoption pressures and strategies in other contexts. This can also extend to soliciting lessons from Norway as a developed-world country for use by those developing-world countries that are still immature to some extent, yet who are willing to innovate with CC in their public sector.

References

Andino A. 2013. 'JottaCloud Review'. *cloudwards.net*. Available at: http://www.cloudwards.net/jottacloud/.

Baldwin H. 2012. 'Public-sector Cloud Computing: The Good, the Bad and the Ugly'. *Computer World*. Available at: http://www.computerworld.com/article/2503858/cloud-computing/public-sector-cloud-computing--the-good--the-bad-and-the-ugly.html.

Bilbao-Osorio B. et al. 2013. 'The Networked Readiness Index 2013: Benchmarking ICT Uptake and Support for Growth and Jobs in a Hyperconnected World'. *World Economic Forum*. Available at: http://www3.weforum.org/docs/GITR/2013/GITR_Chapter1.1_2013.pdf.

Broberg J., Buyya R, and Tari Z. 2009. 'MetaCDN: Harnessing "Storage Clouds" for High Performance Content Delivery'. *Journal of Network and Computer Applications*, 32(5): 1012–1022.

Buyya R. et al., 2009. 'Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility'. *Future Generation Computer Systems*, 25(6): 599–616.

CA Technologies. 2013. *TechInsights Report: Cloud Succeeds. Now What?*. Available at: http://www.ca.com/us/~/media/Files/whitepapers/techinsights-report-cloud-succeeds.pdf.

Cisco. 2013. Cisco Global Cloud Index Supplement: Cloud Readiness Regional Details. Available at: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/CloudIndex_Supplement.pdf.

Currie W. 2009. 'Contextualising the IT Artefact: Towards a Wider Research Agenda for IS Using Institutional Theory'. *Information Technology & People*, 22(1): 63–77.

Currie W.L. 2004. 'The Organizing Vision of Application Service Provision: A Process-oriented Analysis'. *Information and Organization*, 14(4): 237–267.

Currie W.L. and Guah M.W. 2007. 'Conflicting Institutional Logics: A National Programme for IT in the Organisational Field of Healthcare'. *Journal of Information Technology*, 22(3): 235–247.

Darke P., Shanks G. and Broadbent M. 1998. 'Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism'. *Information Systems Journal*, 8(4): 273–289.

Datatilsynet. 2012. *Use of Cloud Computing Services*. Available at: https://www.datatilsynet.no/English/Publications/cloud-computing/.

Devoteam daVinci. 2011. *Felles IKT-utvikling i Kommunal Sektor*. Available at: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Davinci_Felles_IKT-utvikling_kommunal_sektor.pdf.

DiMaggio P. and Powell W. 1983. 'The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields'. *American Sociological Review*, 48(2): 147–160.

EN. 2012. *Unleashing the Potential of Cloud Computing in Europe*. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

Essers L. 2012. 'Norway Ends Nine-month Ban on Google Apps Use'. *Computerworld*. Available at: http://www.computerworld.com/s/article/9231738/Norway_ends_nine_month_ban_on_Google_Apps_use.

Etro F. 2009. 'The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe'. *Review of Business and Economics*, 54(2): 179–208.

Evry 2014. *Cloud Services*. Available at: https://www.evry.com/services/focus/cloud/ [Accessed January 1, 2014].

Frelle-Petersen L. et al. 2012. *Nordic Public Sector Cloud Computing – A Discussion Paper*. Available at: http://www.norden.org/en/publications/publikationer/2011-566.

Garg S.K., Versteeg S. and Buyya, R. 2013. 'A Framework for Ranking of Cloud Computing Services'. *Future Generation Computer Systems*, 29(4): 1012–1023.

Garrison G., Kim S. and Wakefield R.L. 2012. 'Success Factors for Deploying Cloud Computing'. *Communications of the ACM*, 55(9): 62–68.

Gould J., 2012. Interview with the Norwegian Data Protection Commissioner. Available at: http://safegov.org/2012/11/23/interview-with-the-norwegian-data-protection-commissioner.

Haeberlen T., Liveri D. and Lakka, M. 2013. *Good Practice Guide for Securely Deploying Governmental Clouds*. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds.

Hawkins J., 2013. 'Will all Government Services Take a Cloud First Approach?' *The Guardian*. Available at: http://www.theguardian.com/media-network/media-network-blog/2013/mar/07/cloud-public-sector-government.

Hustad E. and Olsen D.H. 2012. 'Adoption of Cloud Computing: A Study of Enablers and Inhibitors in a Norwegian Context. *Proceedings of the 9th International Conference on Enterprise Systems, Accounting and Logistics (9th ICESAL 2012)*: 203–217.

Information Economy Report. 2013. *The Cloud Economy and Developing Countries*. Available at: http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf.

Jørgenrud M. 2011. 'Narvik velger Google Apps'. *digi.no*. Available at: http://www.digi.no/868991/narvik-velger-google-apps.

Kristiansen T. 2011. 'Strong Growth in Cloud Computing in Norway'. *Reuters*. Available at: http://www.reuters.com/article/2011/09/07/idUS46774+07-Sep-2011+HUG20110907.

Malladi S. and Krishnan M.S. 2012. 'Cloud Computing Adoption and its Implications for CIO Strategic Focus: An Empirical Analysis'. *Proceedings of 33rd International Conference on Information Systems (ICIS 2012)*: 1–19.

Marston S. et al. 2011. 'Cloud Computing: The Business Perspective'. *Decision Support Systems*, 51(1): 176–189.

Mell P. and Grance T. 2011. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Microsoft. 2013. *Telenor Uses Windows Azure Virtual Machines for Fast, Efficient, Cost-saving Development and Testing of Company-wide SharePoint 2013 Platform*. Available at: http://www.microsoft.com/casestudies/Microsoft-Azure/Telenor-Group/Telenor-Uses-Windows-Azure-Virtual-Machines-for-Fast-Efficient-Cost-saving-Development-and-Testing-of-company-wide-SharePoint-2013-Platform/710000002349.

Mignerat M. and Rivard S. 2009. 'Positioning the Institutional Perspective in Information Systems Research'. *Journal of Information Technology*, 24(4): 369–391.

Ministry of Local Government and Modernization. 2013. *Digital Agenda for Norway: ICT for Growth and Value Creation*. Available at: http://www.regjeringen.no/en/dep/kmd/documents/white/ propositions/2012-2013/meld-st-23-20122013-2/4/4.html?id=729035.

Morgan L. and Conboy K. 2013. 'Factors Affecting the Adoption of Cloud Computing: An Exploratory Study'. *Proceedings of the 21st European Conference on Information Systems (ECIS 2013)*: 1–13.

Moss Kommune. 2013. *IT-tjenester i Skya?* Available at: http://kunnskapsbyen.no/userfiles/files/Terje Jensen Moss kommune(1).pdf.

O'Donoghue C. 2012. 'The Norwegian Data Protection Authority Holds off Ban, Permitting the Use of Cloud Computing Services by Norway Municipalities'. *Global Regulatory Enforcement Law Blog*. Available at: http://www.globalregulatoryenforcementlawblog.com/2012/10/articles/ data-security/the-norwegian-data-protection-authority-holds-off-ban-permitting-the-use-of-cloud-computing-services-by-norway-municipalities/.

Oliver C. 1991. 'Strategic Responses to Institutional Processes'. *Academy of Management Review*, 16(1): 145–179.

Orlikowski B.W.J. and Barley S.R. 2001. 'Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other?' *MIS Quarterly*, 25(2): 145–165.

Orlikowski W.J. and Baroudi J.J. 1991. 'Studying Information Technology in Organizations: Research Approaches and Assumptions'. *Information Systems Research*, 2(1): 1–28.

Owens D. 2010. 'Securing elasticity in the cloud'. *Communications of the ACM*, 53(8): 1–7.

Palinkas L. A. et al. 2013. 'Purposeful sampling for qualitative data collection and analysis in mixed method implementation research'. *Administration and Policy in Mental*, 1–12.

Paquette S., Jaeger P.T. and Wilson S.C. 2010. 'Identifying the Security Risks Associated with Governmental Use of Cloud Computing'. *Government Information Quarterly*, 27(3): 245–253.

Patton M.Q. 1990. *Qualitative Evaluation and Research Methods*. Available at: http://psycnet.apa.org/psycinfo/1990-97369-000 [Accessed March 4, 2015].

Ragowsky A. et al. 2014. 'Do Not Call Me Chief Information Officer, but Chief Integration Officer: A Summary of the 2011 Detroit CIO Roundtable. *Communications of the Association for Information Systems*, 34(1). Available at: http://aisel.aisnet.org/cais/vol34/iss1/69.

Schneider S. and Sunyaev A. 2014. 'Determinant Factors of Cloud-sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing'. *Journal of Information Technology*, 1–31. Available at: http://www.palgrave-journals.com/doifinder/10.1057/jit.2014.25.

Schwab K. and Eide E.B. 2014. *The Global Information Technology Report 2014 Rewards and Risks of Big Data*. Available at: http://www3.weforum.org/docs/WEF_GlobalInformation Technology_Report_2014.pdf.

Schwab K. and Greenhill R. 2012. *The Global Information Technology Report 2012: Living in a Hyperconnected World*. Available at: http://www3.weforum.org/docs/ Global_IT_Report_ 2012.pdf.

Scott W.R. 2001. *Institutions and Organizations*. Thousand Oaks, CA: Sage.

Seddon J.J.M. and Currie W.L. 2013. 'Cloud Computing and Trans-border Health Data: Unpacking U.S. and EU Healthcare Regulation and Compliance'. *Health Policy and Technology*, 2(4): 229–241.

Shin D.-H. 2013. 'User Centric Cloud Service Model in Public Sectors: Policy Implications of Cloud Services'. *Government Information Quarterly*, 30(2): 194–203.

Su N. et al. 2009. 'Shared Services Transformation: Conceptualization and Valuation from the Perspective of Real Options'. *Decision Sciences*, 40(3): 381–402.

Sultan N. 2010. 'Cloud Computing for Education: A New Dawn?' *International Journal of Information Management*, 30(2): 109–116.

Telenor. 2013. *The Cloud Meets Fibre Optic Broadband*. Available at: http://www.telenor.com/media/press-releases/2013/the-cloud-meets-fibre-optic-broadband/.

Thon B.E. and Vetland S.E., 2012. *Notification of Decision – New e-mail Solution within Narvik Local Authority (Narvik Kommune) – Google Apps*. Available at: http://www.datatilsynet.no/Global/english/2012_narvik_google_eng.pdf.

Venters W. and Whitley E.A. 2012. 'A Critical Review of Cloud Computing: Researching Desires and Realities'. *Journal of Information Technology*, 27(3): 179–197.

Veum H. and Nymoen L.-O. 2012. *Reply - Use of Microsoft Office 365 Cloud Computing Services - Municipality of Moss*. Available at: http://www.datatilsynet.no/Global/english/12 0699 Datatilsynet-Moss kommune-en.pdf.

Veum H. and Thoreid R. 2012. *Case Closed - New e-mail Solution for the Municipality of Narvik - Google Apps*. Available at: https://www.datatilsynet.no/Global/english/12 0699 Datatilsynet-Narvik kommune-en.pdf.

Weerakkody V., Dwivedi Y.K. and Irani Z. 2009. The Diffusion and Use of Institutional Theory: A Cross-disciplinary Longitudinal Literature Survey. *Journal of Information Technology*, 24(4): 354–368.

Wiredu G.O. 2010. 'An Institutional Perspective on the Challenges of Information Systems Innovation in Public Organisations'. *Proceedings of the IFIP International Federation for Information Processing*: 97–108.

Wooten M. and Hoffman A.J. 2008. 'Organizational Fields: Past, Present and Future'. In R. Greenwood et al., eds. *The SAGE Handbook of Organizational Institutionalism*. Thousand Oaks: Sage.

Wyld D. 2009. *Moving to the Cloud: An Introduction to Cloud Computing in Government*. Available at: http://www.ukeig.org.uk/sites/default/files/WyldCloudReport_0.pdf [Accessed November 18, 2014].

Xledger. 2014. *Kundehistorier*. Available at: http://xledger.no/hva-sier-vare-kunder/.

Yang H. and Tate M. 2012. 'A Descriptive Literature Review and Classification of Cloud Computing Research'. *Communications of the Association for Information Systems*, 31(2): 35–60.

Yin R.K. 2009. *Case Study Research: Design and Methods*. London: Sage.

Zhao F. et al. 2013. 'Exploring Cloud Computing Adoptions in Public Sectors: A Case Study'. *GSTF Journal on Computing*, 3(1): 42-27.

Zissis D. and Lekkas D. 2011. 'Securing E-government and E-voting with an Open Cloud Computing Architecture'. *Government Information Quarterly*, 28(2): 239–251.

Understanding Cloud Computing Adoption Issues: A Delphi Study Approach

Corresponding author:
Rania El-Gazzar
PhD Candidate in the Department of Information Systems
University of Agder, Kristiansand, Norway
E-mail: rania.f.el-gazzar@uia.no

Co-authors:
Eli Hustad
Associate Professor in the Department of Information Systems
University of Agder, in Kristiansand, Norway
E-mail: eli.hustad@uia.no

Dag H. Olsen
Professor of Information Systems in the Department of Information Systems
University of Agder, Kristiansand, Norway.
E-mail: dag.h.olsen@uia.no

Abstract

This research paper reports on a Delphi study focusing on the most important issues enterprises are confronted with when making cloud computing (CC) adoption decisions. We had 34 experts from different domain backgrounds participated in a Delphi panel. The panelists were IT and CC specialists representing a heterogeneous group of clients, providers and academics, divided into three subpanels. The Delphi procedure comprised three stages: brainstorming, narrowing down and ranking. The panelists identified 55 issues of concerns in the first stage, which were analyzed and grouped into ten categories: security, strategy, legal and ethical, IT governance, migration, culture, business, awareness, availability and impact. The top 18 issues for each subpanel were ranked, and a moderate intrapanel consensus was obtained. Additionally, 16 follow-up interviews were conducted with the experts to get a deeper understanding of the issues and why certain issues were more significant than others. The findings indicate that security, strategy and legal and ethical issues are the most important. The discussion resulted in highlighting certain inhibitors and drivers for CC adoption into a framework. The paper is concluded with key recommendations with focus on change management, competence and maturity to inform decision-makers in CC adoption decisions.

Keywords

Cloud computing; adoption; Delphi method; decision-making; IT outsourcing; Snowden effect; cloud computing adoption drivers; cloud computing adoption inhibitors

1. Introduction

Recently, enterprises have shown increasing interest in the adoption of cloud computing (CC) services to support critical business functions. According to Luftman et al. (2012), CC is among the five most influential technologies on a global basis, and was considered to be the third most significant IT investment in 2013 (Kappelman & McLeon 2013). The CC market is growing; according to a recent McKinsey report, 60% of small and medium-sized enterprises (SMEs) have already purchased at least one cloud service, and 30% have purchased five or more cloud services (Avrane-Chopard et al. 2014).

CC offers unique capabilities for companies, which can quickly move into a competitive position and take advantage of service-based IT solutions at a low cost. This utility provides opportunities for companies to globalize their processes rapidly, and distributed business operations become easier to perform (Iyer & Henderson 2010; Iyer & Henderson 2012). With decreased costs and less effort required to invest in and maintain the hardware and software, enterprises have more time to focus on their core business activities (Garrison et al. 2012). Additionally, CC services offer features such as elasticity and scalability, which increase the flexibility and agility to undertake the necessary business changes that are required in an innovative and high-competitive environment (Venters & Whitley 2012).

Although several benefits of CC are well known and documented, enterprises are still concerned about the risks and consequences of moving business-critical applications to the cloud. For instance, the distributed nature of CC leads to many different issues, including security and privacy threats, national and international regulations, and the external business environment in which the enterprise operates (Armbrust et al. 2010; Kern, Kreijger, et al. 2002; Marston et al. 2011). A main critique of CC is that the security cost, and the privacy and availability concerns may outweigh its benefits (Kshetri 2013). Several surveys have concluded that the security issue in particular is the most serious barrier to CC adoption within enterprises (Kshetri 2013; Cloud Security Alliance 2013), and consequently, research studies from computer science have focused primarily on different technical issues in terms of security issues and threats (Hashizume et al. 2013; Dorey & Leite 2011; Zissis & Lekkas 2012). Moreover, reliability and trust is emphasized as a barrier in particular for SMEs (Gupta et al. 2013), and compatibility issues (e.g., vendor interoperability, connectivity to existing technology, inter-organizational connectivity) have been identified as an adoption inhibitor (Cegielski et al. 2012; Schneider & Sunyaev 2014; Stieninger et al. 2014).

However, while there are studies that have focused on technological aspects regarding CC implementation (Brender & Markov 2013; Mcgeogh & Donnellan 2013; Garg et al. 2013), the decision regarding whether to adopt CC solutions is additionally complicated by a number of strategic issues (Schneider & Sunyaev 2014). Several studies have pointed out that there is a lack of knowledge and empirical evidence regarding which issues are most important for CC adoption decisions (Schneider & Sunyaev 2014; Yang & Tate 2012). Our research study seeks to contribute to this literature gap, and our research focus is threefold. First, the purpose of this study was to identify the most important issues related to CC adoption decisions in enterprises. Second, we wanted to determine the relative significance of the identified issues. Third, we wanted to elaborate on *why* these identified issues were important.

Due to the nature of our problem, we decided to utilize the Delphi method. This particular research method is appropriate for "identifying and prioritizing issues for managerial decision-making" (Okoli & Pawlowski 2004, p.1), and 34 experts constituted the Delphi panel in this

study. Moreover, we combined our Delphi study results with follow-up interviews with some of the panelists. This methodological approach was appropriate for this study and provided opportunities to achieve a broad overview of CC adoption issues and stakeholders' priorities. The following three research questions (RQs) guided this research:

RQ1: What issues confront enterprises when adopting CC services?

RQ2: What is the relative importance of these issues?

RQ3: Why are these issues important?

The remainder of the paper is organized as follows. First, we present some key concepts of CC and the background and motivation for why this research is needed. Thereafter, the methodological approach is introduced, followed by the presentation and discussion of the results. Finally, further implications for research, practice, and management are identified.

2. **Background**

According to the National Institute of Standards and Technology (NIST), CC is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance 2011, p.2). The current CTO of Cisco described cloud service models, saying, "I see it as three layers: SaaS (software-as-a-service), which delivers applications such as Google Apps and Salesforce.com; PaaS (platform-as-a-service), which provides foundational elements for developing new applications; and IaaS (infrastructure-as-a-service), which is what Amazon has led with, showing that infrastructure can also be accessed through the cloud" (Creeger 2009, p.52).

There are several deployment models for cloud computing (Mell & Grance 2011). In a *public cloud*, the technology is available to all or adapted to a certain industry. A *private cloud* can be created for a particular company and can be operated by the organization itself or outsourced to other suppliers. In a *community cloud*, the cloud infrastructure is limited to a specific community of consumers from organizations that may have shared demands (e.g., security requirements, policy, and compliance considerations). In a *hybrid cloud*, public and private cloud services are combined.

It was foreseen that, by 2015, businesses will be more oriented towards agility (Andriole 2012). CC was speculated to be among technology trends that will define how organizations acquire, deploy, and maintain information technology (IT) in the future, and the concern for researchers has to focus on "what are the obstacles to cloud adoption, rank-ordered by concern, cost, and impact?" (Andriole 2012, p.68). CC has recently received increased attention from the IS research community (Lacity & Reynolds 2014; Venters & Whitley 2012; Chen & Wu 2012; Loebbecke et al. 2012; Galliers et al. 2012). However, the issues and the implications of CC are still poorly understood (Luftman et al. 2012), and CC is yet an immature research area (Lacity & Reynolds 2014; Lacity et al. 2010). With the increasing development of service models for IT delivery and businesses' interest in such models, scholars are encouraged to contribute to "advancing the knowledge base on phenomena related to IT-based services" (Fielt et al. 2013, p.46).

Thus, there are several reasons that have motivated our research on CC adoption. First, IS researchers have recommended several future research directions to gain more knowledge about the benefits and challenges of CC. These recommendations encompass CC economics, strategy and policy issues, technology adoption and implementation issues, regulatory issues, among others (Marston et al. 2011), and focus on the service dimensions of the cloud in terms of efficiency, creativity, and simplicity (the cloud's desires) (Venters & Whitley 2012).

Second, we position our research as a contribution to IS studies on IT services, which have recently received an increased attention in both academia and industry (e.g., increased focus on service-oriented architecture (SOA), web services, and CC). Thus, there has been a call for more research to advance the knowledge base on phenomena related to IT services, including CC (Fielt et al. 2013). Future research needs to take on an interdisciplinary perspective to add knowledge to the science of service by exploring the value of CC across different industries. This involves studying economic, technical, and organizational issues of CC adoption (Bardhan et al. 2010).

Third, as CC represents a paradigm shift from traditional IT outsourcing (ITO) to netsourcing (Dibbern et al. 2004; Susarla et al. 2003; Kern, Lacity, et al. 2002), the ITO literature has prompted research that focuses on IT delivery as a service and has suggested future research directions for CC (Lacity et al. 2010; Lacity et al. 2009; Schneider & Sunyaev 2014). The existing body of research on ITO provides an appropriate foundation for investigating cloud-sourcing decisions (Muhic & Johansson 2014). However, while traditional ITO shares common characteristics with cloud sourcing, there is a need to gain a broader understanding of specific features and strategic issues of CC as a sourcing model, which traditional ITO solutions do not possess (Schneider & Sunyaev 2014; Malladi & Krishnan 2012). In order for businesses to maximize their benefits from adopting CC services, they need to consider three key elements: potential risks, opportunities, and challenges (Marston et al. 2011). Therefore, the challenge for businesses is to "strategically decide whether and how to pursue various service transformation" (Su et al. 2009, p.381). This puts the responsibility on executives to "have extensive judgment and insight regarding organizational structures, interdependencies, processes, and habits to thoroughly comprehend decision alternatives and the set of required structural choices" (Schneider & Sunyaev 2014, p.1). Thus, there is a need for further research regarding strategic motivations, internal and environmental influences, and dynamic interactions between these influences (Schneider & Sunyaev 2014; Lacity et al. 2010).

With regard to the abovementioned backdrop, there is a need for more empirical research to explore and to advance our knowledge on the issues that are of most concern when enterprises consider adopting CC services. This is necessary to provide guidelines for decision-makers in enterprises considering migration to CC services.

3. **Research Method**

This study primarily aimed to reveal the most important issues that enterprises would need to consider in their decision-making process regarding adoption of CC services. To this end, we adopted principles from the Policy Delphi method, which would be appropriate for exploring a complex topic to generate ideas and judgments from experts (Franklin & Hart 2007). Moreover,

the Delphi procedure is "a rapid and efficient way to cream the tops of the heads of a group of knowledgeable people" (Dalkey 1972, p.16). The second purpose was to prioritize the issues of most concern by conducting a "ranking-type" Delphi study (Schmidt 1997). The Delphi approach is recognized and utilized among IS researchers on a variety of IS topics (Schmidt 1997; Iden et al. 2011; Keil et al. 2013; Akkermans & Bogerd 2003).

3.1. Delphi Study Design

We designed the study by following the principles and guidelines documented in the Delphi literature to ensure rigor, validity, and credibility (Franklin & Hart 2007; Okoli & Pawlowski 2004; Day & Bobeva 2005; Schmidt et al. 2001). We conducted a ranking-type Delphi study that involved a sequential set of steps: (1) brainstorming, (2) narrowing down, and (3) two rounds of ranking (Schmidt 1997). The ranking part of the study was vital for building consensus within the panel (Hsu & Sandford 2007); the consensus was attained by reaching an agreement regarding the most important CC adoption issues for each distinct group of panelists. In addition, we conducted follow-up interviews with 16 of the panelists. The purpose of the interviews was to enrich and contextualize the existing data to turn "thick descriptions" into stronger conclusions by triangulation (Myers & Newman 2007).

To set up a Delphi panel, we searched for practitioners with considerable IT expertise and at least three years of experience, in addition to being involved with CC at their workplaces. Our sources were literature (both academic articles and practitioners' articles), LinkedIn, and reference contacts. Invitations were initially sent to 60 experts, of whom 34 accepted. The participants represented a heterogeneous group and were further divided into three subpanels comprised of 17 providers, 12 clients, and 5 academics. They were selected from different countries (6), industries (13), company types (public or private), company sizes (large, SME, and micro), and organizational roles (5) (See Table 1 for an overview). This variety provided the opportunity to obtain diverse opinions on CC adoption issues. The involvement of practitioners and academic experts was helpful, and it facilitated a better understanding of various issues of concern about the phenomenon (Ward 2012). Academic experts were interested in participating, as they were involved in field studies regarding CC adoption. Clients who were early, recent, or potential adopters of CC services were interested in sharing their experiences and concerns about CC. The providers represented different companies including IT vendors, cloud service providers (CSPs), cloud service brokers, and IT consultancy firms, all of whom were interested in sharing experiences and obtaining viewpoints from clients, including potential customers.

During the study, communication with experts took place remotely via email for convenience, and all questionnaires and results were emailed separately to each expert, thus guaranteeing full anonymity to the experts. Subject anonymity reduced the effect of dominant individuals. Additionally, statistical analysis was employed to reduce group pressure for conformity and to ensure that each expert's answer was well represented in the final round (Dalkey 1972).

Table 1: Composition of the subpanels (*3 (A): A3, A2, A1—three experts from the Academic subpanel (A); their codes are A3, A2 and A1. **1 (P): P13—one participant from the Provider subpanel (P); his code is P13. ***1 (C): C12—one participant from the Client subpanel (C); his code is C12.)

Industry/Size/Type			Job Category/Country											
			Senior Management				Middle Management				Technical Profession		Senior Consultants	Academic Scholars and Lecturers
			NOR	USA	UK	PK	NOR	FIN	EGY	PK	NOR	EGY	NOR	NOR
Education		Public												*3 (A): A3, A2, A1
		Private												1 (A): A4
Research		Private												1 (A): A5
Information Technology and Services	Large	Private	2 (P): P4, P2										3 (P): P12, P16, P17	
	SME	Public							1 (P): P14					
		Private		1 (P): P1			**1 (P): P13							
	Micro	Private			1 (P): P5									
Education Management	Micro	Private	1 (P): P3											
Management Consulting and IT Outsourcing	Large	Private	1 (P): P10								1 (P): P8			
Accounting	SME	Private	1 (P): P9											
Telecommunications	Large	Private				1 (C): C1		1 (P): P15		1 (C): C5		***1 (C): C12		
	SME	Private		1 (P): P11										
Government Administration	Large	Public	2 (C): C2, C4				1 (C): C10							
	SME	Public	1 (C): C8				1 (C): C6							
Healthcare	Large	Public					1 (C): C3							
Oil and Gas	Large	Private	1 (C): C7											
Power	Large	Private					1 (C): C9							
Chemicals	Large	Private	1 (C): C11											

Computer Software	**SME**	**Private**	1 (P): P6				1 (P): P7							

3.2. Data Collection and Analysis

Figure 1 summarizes the overall research process comprising the Delphi phases and follow-up interviews. Each phase is described subsequently in details followed by the interviews.

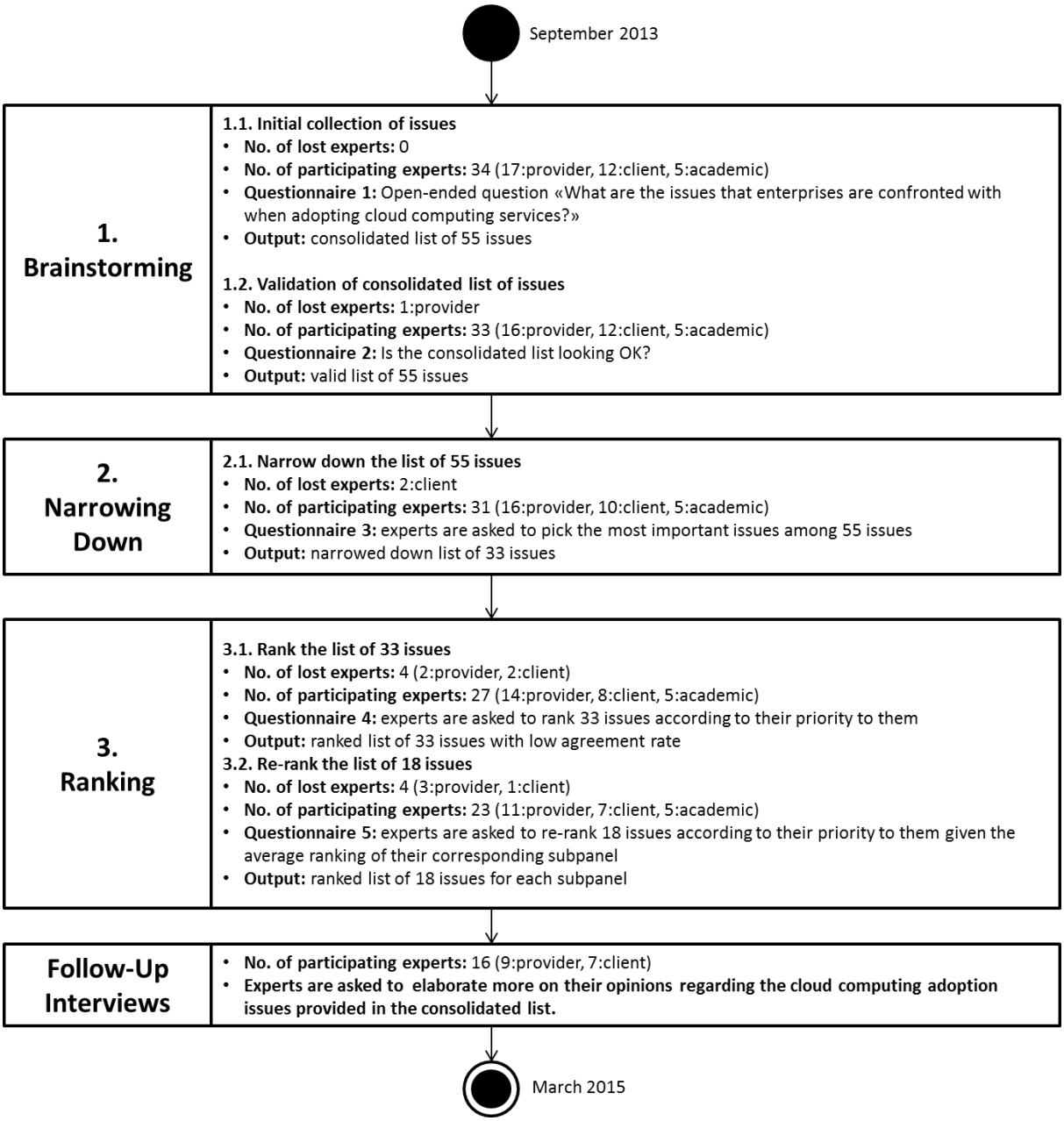


Figure 1: Summary of the Delphi phases and follow-up interviews

3.2.1. The Brainstorming Phase

In the brainstorming phase, an open-ended question was sent to each of the experts by email: "What are the issues that enterprises are confronted with when adopting cloud computing services?" We asked them to provide at least six issues to answer our question as well as to define each issue, justify its importance and consequences, and if possible, add comments for

elaboration. Based on the experts' statements and explanations, the authors of this paper analyzed the generated material. The analysis sought to identify the most important issues; through this work, similar issues were combined, and duplicate meanings were removed. In total, 55 different issues were identified, further systemized, and grouped into 10 main categories which were determined as critical for cloud computing adoption in organizations: (1) security, (2) legal and ethical, (3) business, (4) cultural, (5) availability, (6) awareness, (7) impact, (8) strategy, (9) migration, and (10) IT governance. The experts validated the list generated at this stage by reviewing the list to ensure that all their issues were included, analyzed, and interpreted correctly by the researchers. Table A in the Appendix depicts the list of 55 issues identified by the panel.

3.2.2. The Narrowing-Down Phase

In this phase, we asked the experts to select 10 (minimum) to 20 (maximum) issues that they believed were most important to them. Each expert received a randomly arranged list of issues to avoid bias in the listing order of the items (Okoli & Pawlowski 2004). We chose to analyze each subpanel separately and noticed differences among the subpanels in prioritizing the issues. Thus, we wanted to highlight these differences in addition to analyzing the combined panel's results. First, we calculated the percentage of total votes gained for each issue by each subpanel. The purpose was to narrow down the list of issues into a manageable size of 15 items at least and 20 at most. With this in mind, we utilized the strategy of selecting issues that were chosen by over 50% of the participants in each subpanel. This produced an overly short list of 12 issues out of 55. Our concern was that the list of issues was too narrow, and we needed to be careful not to overlook other important issues that had votes slightly lower than 50% in each subpanel. Therefore, we decided to utilize 30% as a possible threshold to consider the most important issues for experts in each subpanel. This resulted in a list of 33 issues ready for ranking. Since the experts (not the researchers) were the ones deciding on the most important issues (Schmidt 1997), we decided not to utilize any arbitrary method to further reduce the number of issues.

By comparing the results of the brainstorming stage (identification of issues) with those of the narrowing-down phase (selection of most important issues), the reduction analysis provided: (1) security (identified = 14 issues, selected = 11 issues), (2) availability (identified = one issue, selected = one issue), (3) migration (identified = three issues, selected = three issues), (4) business (identified = nine issues, selected = two issues), (5) legal and ethical concerns (identified = seven issues, selected = five issues), (6) culture (identified = two issues, selected = one issue), (7) awareness (identified = four issues, selected = one issue), (8) impact (identified = seven issues, selected = five issues), (9) IT governance (identified = one issue, selected = one issue), and (10) strategy (identified = seven issues, selected = three issues).

3.2.3. The Ranking Phase

In this phase, a randomly arranged list of 33 issues was sent to each of the experts for ranking. The purpose was to determine the relative importance of the issues. To measure the degree of consensus among the experts in each subpanel, we calculated the mean ranking and Kendall's coefficient of concordance (*W*) for each subpanel. The value of Kendall's *W* provides a measure

of the consensus among the panel participants (Kendall & Gibbons 1990). We could not reach the level of concordance of $W = 0.7$ that is considered to be an indication of a high level of agreement for Delphi studies (Schmidt 1997). (A Kendall $W = 1.0$ means full agreement in the panel regarding the order of the ranked issues). The Kendall W values showed low and insignificant agreement for all three subpanels: academics (N = 5 academics, $W = 0.270$, sign = 0.089), clients (N = 8 clients, $W = 0.173$, sign = 0.072), and providers (N = 14 providers, $W = 0.069$, sign = 0.533). See Table B in the Appendix for details on the rankings of 33 issues.

We decided to conduct a new ranking round, aiming to increase Kendall's W to be more precise regarding *the relative importance* among the issues identified. The first round gave us an indication of which of the 33 issues was most important, and it was then easier to reduce the number of issues. We decided to focus on the top 18 issues, based on the mean ranking for each subpanel. The feedback from the first round of ranking gave us an impression of the difficulties in ranking too many issues, so by reducing the number of issues, it would be easier for the panelists to focus on the most important issues for them. Since each subpanel had ranked the 33 issues quite differently, it was important to keep the subpanels separate and focus on the top 18 issues for each subpanel.

Afterwards, we calculated the mean ranking and Kendall's W values for each panel. Despite we reached a moderate degree of consensus, we decided to stop the rounds of ranking at this stage. The study had already exceeded its original time schedule, since each step had taken longer than expected, and several reminders had been sent to the panelists. Moreover, we had lost experts during the study (See Figure 1); thus, we expected that starting a new round of ranking would decrease the number of experts even further and, consequently, reduce the validity of the results. The last round of ranking had only led to minor adjustments to the rankings of each subpanel, and for practical purposes, performing another round would not be necessary. We also conjectured that the follow-up interviews would provide more insight and, thus, be more valuable.

3.2.4. The Follow-Up Interviews

As previously indicated, the purpose of the interviews was to enrich and contextualize the existing data achieved from the Delphi study. Follow-up interviews were an important means to triangulate our results from the Delphi study and thereby increase the validity of the data in the study (Day & Bobeva 2005). All panelists were invited to participate in a follow-up interview, and 16 panelists agreed. Table 2 below provides an overview of the interviews that were conducted.

The interviews focused on the issues that the individual panelist had highlighted during the brainstorming phase. Additionally, the list of 33 issues representing each subpanel's perspective on CC adoption issues after the first-ranking round was discussed with each interviewee. The interviews gave the experts the opportunity to elaborate on their individual opinions about CC adoption issues and to further clarify the consolidated list of issues. Some of the interviewees also tried to explain the differences across the subpanels. The interviews were conducted in parallel with the ranking phase.

Table 2: Overview of the interviews

No.	Expert code	Company type	Expert position	Years of experience		Mode of communication	Duration	Interview date
				IT	Cloud			
1	P16	Consultancy	Senior consultant	10+	2+	Face-to-face	1 hour : 29 min	23rd May 2014
2	P2	Vendor	Director cloud computing	30	3	Face-to-face	1 hour : 17 min	28th May 2014
3	C1	Client	Director global IT services	10+	4	Online	34 min	29th May 2014
4	P4	Vendor and consultancy	Offer director for cloud transformation	17	4	Face-to-face	1 hour	6th June 2014
5	P1	Cloud service broker	Vice president & General manager cloud services	20+	5+	Phone	28 min	10th June 2014
6	C4	Client	CIO	15	3	Phone	23 min	18th June 2014
7	P13	Cloud provider and vendor	Product manager	16	5	Face-to-face	56 min	24th June 2014
8	P15	Cloud provider/vendor/ and consultancy	Business development manager	15	2	Face-to-face	54 min	26th June 2014
9	P7	Vendor	Product and R&D manager	20	10	Face-to-face	37 min	12th August 2014
10	P12	Consultancy	Senior Consultant, team lead CRM / Cloud Advisory	5	5	Online	32 min	14th August 2014
11	C3	Client	Lead Enterprise Architect	23	2	Online	44 min	15th August 2014
12	C10	Client	IT Advisor	20	1	Face-to-face	44 min	22nd August 2014
13	C8	Client	CIO	9	2	Phone	25 min	26th August 2014
14	P6	Cloud provider and vendor	CEO	15	7	Online	53 min	29th August 2014
15	C12	Client and cloud provider	Cloud infrastructure administrator	5+	2+	Online	37 min	29th August 2014
16	C2	Client	Vice president	21	6 m*	Face-to-face	42 min	15th August 2014

* It has been six months since the expert LS started to investigate the possibilities and consequences of using CC. LS has not started using it, but is in the stage of proofing the concept.

4. Results

4.1. Final Results of the Delphi Study

Table 3 depicts the results of the second round of ranking, which determined the relative importance of the top 18 issues for each subpanel. The relative importance of 18 issues was ranked differently among the subpanels. The critical issues which constitute each category provide information that may assist the decision of CC adoption. According to the panelists of this study, these are the issues that CC adopters should consider the most in CC decision situations.

In general, there was an improved degree of agreement within each subpanel compared to the first ranking results. The highest Kendall's *W* was among the academics (N = 5 academics, *W* = 0.493, sign = 0.001). However, there was an improved and significant (though not high) degree of agreement among the clients (N = 7 clients, *W* = 0.392, sign = 0.000) and the providers (N = 11 providers, *W* = 0.443, sign = 0.000). Consequently, each subpanel showed a moderate degree of consensus according to Kendall's *W*, which was in the 0.4–0.5 range. This indicated a moderate intrapanel agreement for all three subpanels.

The ranking results show that the dominant issues are related to four specific categories; security, strategy, and legal and ethical concerns, and IT governance (e.g., among the top nine issues for all the subpanels). We found that the client panel ranked the issue "Data protection legislations are different and not strong in all countries" as number one, the provider panel ranked the issue "The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that in public clouds. However, risks are not absolute, and most of them can be addressed, but not all of them" as number one, and the academic panel ranked the issue "Enterprises are faced with weak undetailed Service Level Agreements (SLAs) from providers (e.g., providers may not be transparent about where and how do they store the data and the acknowledgement of security incidents whenever happen and how the cloud provider deals with it)" as number one.

By examining the combined ranking (CR) results, we see that both clients (C) and academics (A) highlight the risk of relying on external CSPs if problems with the technology arise. This may lead to less control and may decrease the performance of business functions when problems occur (CR = 15; C = 9, P = not ranked (÷), A = 8). The providers (P) particularly emphasized the categories of culture (CR = 11; C = ÷, P = 6, A = ÷), IT governance (CR = 9; C = 17, P = 8, A = 17), and migration (CR = 14; C = ÷, P = 9, A = ÷). Culture represents a social dimension in the dataset and resistance to change should not be underestimated as a challenge when implementing cloud computing; providers P1 and P4 emphasized the urgency of having a plan for cultural changes when implementing new routines and processes that fit with CC. Providers (P1 and P10) argued that several clients lack IT governance practices and skills and, therefore, are not able to manage and maintain CC services in a proper way: "Top management is often reluctant to adopt anything that does not fit within established governance framework/practices" (P10). Consequently, this leads to increased legal jeopardy, excessive costs, and inability to reap the benefits from CC services as provider P1 emphasized. Providers stress that migration between CC services without affecting the current business operations is a very important issue to consider.

The academics (A) ranked the category of impact higher than the other subpanels (CR = 16; C = 16, P = ÷, A = 6). The academics were concerned about potential disruptions of IT and business operations when transitioning from in-house solutions to cloud solutions. Awareness was also ranked high among the academics (CR = 18, C = ÷, P = 18, A = 9); the academics thought that the concept of cloud and its potential value are not well understood by the clients.

Table 3: Ranking results of the top 18 issues for each subpanel, organized by priority of combined ranking

CR*	Issues	C (N = 7)	P (N = 11)	A (N = 5)	Category
1	The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.	3	1	2	Security
2	Data protection legislation is different and not strong in all countries.	1	10	3	Legal and ethical
3	Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.	7	2	12	Strategy
4	There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.	6	3	15	Security
5	It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it must be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.	8	4	10	Strategy
6	Compliance with data privacy Acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.	5	11	4	Legal and ethical
7	Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).	13	13	1	Legal and ethical
8	Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.	2	17	11	Security
9	There is a lack of IT governance tools, policies, and best practices particular to cloud-service management.	17	8	17	IT governance
10	It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects.	15	5	÷	Legal and ethical
11	People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.	÷	6	÷	Culture
12	The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.	÷	7	÷	Strategy
13	The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.	14	15	÷	Migration
14	There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.	÷	9	÷	Migration
15	The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.	9	÷**	8	Impact

16	There is concern about whether the transition to the cloud disturbs current IT and business operations.	16	÷	6	Impact
17	The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.	÷	14	16	Security
18	The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.	÷	18	9	Awareness
19	The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.	4	÷	÷	Security
20	Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.	11	÷	14	Impact
21	Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.	÷	12	÷	Business
22	It is unclear who owns the data.	÷	÷	5	Security
23	Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.	÷	16	÷	Security
24	There may be insufficient and inconsistent data encryption policies and practices.	10	÷	÷	Security
25	It is hard for small clients to modify the standard agreements of major international cloud providers.	÷	÷	7	Legal and ethical
26	If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.	12	÷	÷	Business
27	One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.	18	÷	÷	Security
28	Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.	÷	÷	13	Migration
29	There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity.	÷	÷	18	Availability
	Kendall's *W* Sign.	**0.392 0.000**	**0.443 0.000**	**0.493 0.001**	

*CR = combined ranking (total of 29 issues for all three subpanels).

**The symbol ÷ indicates that the issue was not among the top 18 issues for this particular subpanel.

Our further discussion focuses on the issues that were ranked highest across the three subpanels. The highest ranked issues were from three of the main categories, namely security issues, legal and ethical issues and strategic issues.

4.2 Combining Results from Expert Interviews with the Delphi Results

The interviews supported the findings from the Delphi rankings and provided valuable insights to further examine and understand the issues. In the following subsections, we discuss the most important issues highlighted in the Delphi study comprising information from both the brainstorming phase and the ranking rounds, and which were further elaborated in the interviews. The interviews also highlighted some additional issues related to the maturity of the clients' business processes and enterprise architecture, the maturity of CC services available today, and the political game that runs across the CSPs and traditional IT providers. These additional issues are also discussed. Several issues were found to be overlapping and interrelated. However, for analytical convenience, these issues are presented in turn.

4.2.1 Security Issues

Security related issues dominated the rankings of all the panels, and this was corroborated by the interviews. We address the most significant issues based on the Delphi rankings and the interviews. First, the most important issue overall was "The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them." It was among the top three issues in all the subpanels (C = 3, P = 1, A = 2), and was the most important concern in the interviews.

The experts view the risk of losing control over resources as particularly significant in public clouds, and less so in private clouds. The experts believe that these risks can be addressed to a large extent and, thereby, can be controlled, but at a cost. Clients and providers view this issue from two different perspectives and have different opinions about what constitutes this security problem. Clients perceive this problem as stemming from the risk of information exposure as a weakness in CC, which has not yet been resolved in an appropriate manner. In contrast, most of the providers think that the main problem is the clients' lack of competence and skills in security management.

Clients highlight that security issues may prohibit the adoption of CC, as it is associated with various risks. Clients' concerns about security control relate to confidentiality, integrity, and availability of sensitive information and lack of knowledge as to where the information is stored and replicated. The following remark was stated by client C12 and was typical among clients: "Information is really the most valuable asset of an enterprise [. . .] loss or even threat of loss of information can cause enterprises to fall apart." Several clients noted that security breaches can lead to less competitive advantage and loss of sensitive information, and can affect the brand reputation and company share prices, which can ultimately lead to the loss of a company's trustworthiness.

The interviews showed that CSPs constantly face the clients' concern about security risks. Provider P12 perceived this to be an irrational fear—P12 believes that cloud services are more secure than in-house solutions: "There is some sort of [. . .] irrational fear of moving data from

[the local data centers] into somewhere you don't know where it is. Why I call it irrational is that local data security is seldom more secure than having data stored with the best security providers in the world." Provider P7 corroborated this opinion and argued that the clients may not have the properly skilled IT department that the CSPs have: "It is a kind of two-edged sword because when everything is in-house for instance, [you may think that] you control your own IT department and you also control all the security issues, but that is not true because a lot of the local IT departments do not have skills with regard to security to be able to protect the company as good! So it might be better to look to a vendor that is really skilled on this."

Some providers indicated that there is a political game going on between CSPs and traditional IT providers about whether clients can trust CC solutions or not. The providers claimed that ASPs and traditional IT vendors overstate the CC security challenges to discourage their clients from moving to competing cloud offers. Provider P4 noted that: "It is not easy to be a customer [given the conflicting messages]." Additionally, several providers raised a further issue that is related to the debate between large international CSPs and local CSPs. Large international CSPs have big clients who will take the CSP to the court if there are any security breaches. This is asserted by expert C12 who has worked for a global CSP: "I get more worried about local CSPs who are new in the market. Large international CSPs, [have considered critical security issues], because there is a lot of focus on them. They are dealing with mature customers who have large legal entities, and if there is a flaw in the contract, they will hunt them down". From the provider's point of view, large international CSPs were perceived to be more secure than local and smaller CSPs. Provider P13 asserted the importance of trust in international CSPs, since they are more secure and have invested much in security of their services: "Most important is [trust in] vendor relationship. I think security is higher in the cloud because of the investments that these large vendors have put into security, but I think the perceptions by the customers are different." In contrast, the clients perceive local CSPs to be more secure and compliant with regulations.

Clients believe that local CSPs can be a guarantee that the data would be stored within the client's country. Providers argued that this may not be true, as some CSPs may use third party CSPs to store the data. Provider P4 observed: "Often the 'non-real' CSPs are smaller companies with local presence and focus. Due to the local presence, customers believe it is a safer choice than larger companies with global business and operations. This is a big misunderstanding, because [. . .] they may use third party providers that store data wherever they want." This chain of CSPs makes it difficult to trace whether the legislation and internal security policies are met.

Even if the local CSPs are not using third party CSPs and they store the data locally, they may not be secure enough, as they do not have the competence and expertise in security governance that international CSPs have. This was asserted by provider P12: "If in general you say you would trust a local CSP more than the global one, I would disagree to that! That is more an issue of regulations, so it's easier to understand regulations if you have a [local CSP with a local data center] [. . .] but I wouldn't say it's more secure. The global CSPs are the ones attracting the best security talent, the best developers; they have the best and more secure data centers, and they operate on multiple continents."

Many providers suggested that clients must establish proficient security governance before they will be able to have control over their data. Providers believe that CSP security audits may mitigate some of the CC's security problems. Furthermore, expert C12 advocated the involvement of the security department throughout the migration to the cloud: "The security

department has to be consulted and involved at every step of the migration from the requirements gathering, the technical implementation and until the support cycle is in production and running [. . .]. This is one of the main concerns and obstacles for a full migration to a public cloud."

Many experts believed that private clouds would offer more security than public clouds. However, private clouds are not as efficient as public clouds when it comes to scalability and cost effectiveness. Client C2 had faced this dilemma: "We debated whether we should have a private cloud or we should go to a public cloud, [. . .] maybe a hybrid. Now we are building a private cloud." One of the reasons for opting for a private cloud is that it offers more security than public clouds; private clouds solve the issue of the server's location, as provider P13 pointed out. Provider P12 corroborated this view and added that private clouds are not efficient when it comes to scalability and cost effectiveness.

Secondly, the issue "There is a lack of trust in the cloud's multi-tenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage," was ranked highly by the provider and client subpanels (C = 6, P = 3, and A = 13), and this was supported in the interviews. This issue is also related to the security issues of CC, and focuses particularly on the clients' skepticism towards the shared public CC environment, and that foreign governments are able to access their data.

The hypervisor is the basic component that creates and runs the virtual machines (VMs), which are hosted in a cloud environment. In a public cloud environment, the multi-tenancy model involves having a VM for company X beside a VM for company Y. Several experts noted that this model triggers a challenge for CSPs to keep on segregating VMs of different clients from each other. Provider P7 pointed out that it is important to make sure that the clients are confident that their data is secure to keep increasing their cloud sales and preserving their image in the cloud market: "I believe one scandal in this area might create enormous trouble for the sales of cloud solutions [. . .]. How do we secure bulletproof walls between customers? How separate should systems be? Different databases? Different software? How do we share, but in such a way that the customers are absolutely sure their data is as safe as it is in their own house – but in the cloud?" Thus, if the hypervisor is compromised, it will cause unfavorable consequences for both CSPs (i.e., losing customers) and clients (i.e., hacking and deletion of VMs).

Several providers pointed out another issue related to clients' trust, which is the governments of countries that host the cloud environment; this has become clear, especially since the revelations about NSA actions following the Patriot Act. For example, clients who are operating within the E.U. region would prefer contracting E.U.-based CSPs rather than U.S.-based international CSPs. This is expressed by provider P12: "So I think it is about trusting your data with somebody that you don't know [. . .] NSA actually being able to access your data is the most common security issue, and that is why one of our clients was very satisfied when we have CC providers working within the European Union because that feels safer than moving data overseas."

Provider P13 advised that clients need to consider the worst case of service unavailability, such as that which can be caused by a government investigation: "You have to think about the worst case that can happen. [. . .] In America, for example, they can just open an investigation, and they can freeze the data in the data server and the storage just to go through all of it, and even if

they don't find anything, this can disrupt the business. Do you want to have the data in the country where that would happen, or do you want to have data locally and have full control?"

Thirdly, the issue "Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for." was the second highest ranked issue in the clients' subpanel (C = 2, P = 17, and A = 9). This issue is also about the fundamental security issues, and shows that clients are concerned about the relevance of the CSPs' security compliance with their particular needs. The significance of this issue is illustrated by the following statement by client C1: "It is also challenging that they meet our security protocols, because [. . .] all our applications that are at data centers have to meet a certain level of security standards, and if those security standards in terms of IT security and in terms of physical security are not met, we cannot move or host our applications at those datacenters." Clients may need security requirements more than just having their data within a certain country or certain region; they have security standards related to their specific type of industry, like telecommunications (as in the case of client C1), healthcare, or banking.

Clients have different security concerns, according to the basic information security triad (i.e., confidentiality, integrity, and availability), which are related to the type of industry in which they operate; this was expressed by provider P16: "It depends on the company, what are they doing. [For example, regarding confidentiality:] Coca-Cola, I am not sure if Coca-Cola wants to store how they make Coca-Cola on Google cloud service! I don't think they want to do that, because that information is so precious to them, and that information brings them so much money, and it is so secret that I don't think they will trust Google or Microsoft to store that information - [Regarding integrity:] The stock market, what is important for them is integrity, and that means that nobody is able to change the prices [. . .] If criminal people are able to do it, then they can destroy the market and nobody will trust it - [Regarding availability:] The big deal for the banks is to be available at all times [because most of the transactions are done online]. If one bank is down for one hour, then it is a lot of money—so it is critical!"

4.2.2 Strategic Issues

Several of the top ranked issues were related to the strategy issues category, in addition to also being closely related to the security issues. Firstly, the issue "Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations." was highly ranked by clients and providers (C = 7, P = 2, A = 11), and it relates to the security challenges of hosting data in the cloud and focuses on the challenges related to the interruptions of critical operations. The expert interviews confirmed that this issue was highly significant. Several clients pointed to the need for service availability in certain industries, such as healthcare, which is a critical environment that cannot risk incidents and downtime.

Several experts noted that service unavailability issues can result from accidental events that happen to the network infrastructure itself or due to network upgrading. Accidental events can be road construction, which can cause damage to the cables and lead to a service outage. Such incidents affect critical operations of some organizations and may cost lives. Client C3 asserted: "There was an outage [at one of the hospitals]. The communication switch has been upgraded by the vendor without informing us about it. They did not understand the consequences of this upgrade. This caused the whole hospital to go down. It does not help the patients that we are

arguing about the SLA with the cloud vendor. We have to fix the problem quickly. So when lives are at risk, we have to do the SLA discussion afterwards. So that is why we are a bit paranoid about service levels."

Failure to meet clients' expectations with regard to service availability or rapid CSP responsiveness can also have negative consequences for CSPs; it costs them their trustworthiness. This is expressed by provider P6's comment: "If the system is down, it will hurt every customer connected to the service. You expect 24/7, and downtime is a serious threat to keep on being a customer. This will cost the CSP losing customers and could be downgraded in the marketplace and lead to less confidence."

Secondly, the issue "It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it must be kept on-premise. On the other hand, non-sensitive data and functions can be outsourced to the cloud." was among the top 10 issues across the subpanels (C = 8, P = 4, A = 10), and it is related to the security challenges of hosting data on the cloud or keep it on-premise. Several providers highlighted the need for mature CC models, such as private clouds for hosting sensitive data. Choosing between the cloud and on-premise computing depends on the criticality of the data and applications, and on how much data these applications generate. Client C1 highlighted, for instance, that applications generating a large volume of data and that perform core telecom operations can present a major challenge if they would be outsourced to CSPs: "telecom companies are going on the cloud for applications which are more business oriented applications, and not core telecom operations that generate telecom related data. [. . .] So if, for example, my [Intelligent Network] system, which is a core telecom system, has to be hosted somewhere outside the country with the kind of traffic that we generate in Asian countries [. . .] It would require a high level of bandwidth, and I don't think that this bandwidth can be provided by CSPs."

Thirdly, although not ranked among the top issues, some other interesting issues surfaced during the interviews. These issues related to the maturity of the clients, which we have grouped into the category of strategy. It is important that an adoption strategy take maturity considerations into account. Furthermore, overlooking the degree of maturity for the client organization can decelerate the benefit realization of CC services.

One significant issue related to the maturity of the clients is the maturity of their business processes and enterprise architecture (i.e., standardization). Client C1 asserted the importance of this issue: "The underlying fundamental reason was a strategic drive towards outsourcing and making the internal organization leaner […], but in the entire process we [lacked focus on our cloud readiness]. We are [now outsourcing a couple of applications] to different cloud vendors and we face a lot of integration problems between the cloud solutions and the local legacy solutions. Especially, in a multi-functional and multi-application service environment the problem is related to the maturity of the processes, because one of the basic requirements in the cloud is the 'standardization of processes'. So it is a problem for companies like us which are not mature in terms of standardization."

A number of panelists (six providers and three clients) stressed that clients need a certain maturity in their enterprise architecture in order to be able to integrate public cloud services into their business applications in an appropriate manner. Provider P4 highlighted the need for a

modular architecture to allow for integration with CC services: "I think the most important issue is to understand the architecture and […] if you have a good modular architecture, you can easily see if there are functionalities that [can be put in the cloud]." It was also asserted by a number of panelists that very few client companies are presently at the required maturity level.

A number of panelists also pointed out that cloud efforts need to be linked to the business model. The comment from provider P1 illustrates this: "The real capability of the cloud is in redesigning the business model – and most of the people want to start with technology. And if you have that view, you don't change the business model, and then you can't reap the broad benefits of transitioning to the cloud."

Consistent with this view, several panelists pointed out that clients usually invest in CC services as a local initiative and not as an integral part of the business and IT strategy. Provider P4 asserted this issue: "I think typical sales and marketing, they go directly and buy, for example, Salesforce without involving IT staff in a good way – because IT staff will delay them and just ask questions that take a lot of time to answer."

4.2.3 Legal and Ethical Issues

Three of the top ranked issues relate to data legislation issues. The issue "Data legislation is different and not strong in all countries." recorded high rankings in the three subpanels; and was number one in the clients subpanel (C = 1, P = 10, and A = 3), and it was supported in the interviews. This issue is about the challenge of having to comply with data protection legislation in different countries, which is often inconsistent. This issue gets particularly complicated for client organizations with a global presence. An example case is that of client C1; this client's organization was originally located in the E.U., but they run several subsidiaries around the globe (e.g., Pakistan, India, Bangladesh, etc.). In this case, they have to adhere to E.U. laws regarding data privacy in addition to the fact that each subsidiary has to follow local laws of its country, which in this case is Pakistan, when providing IT services for business units located in different countries. Client C1 observed: "With companies like us, which is based in the E.U., we have a challenge in terms of data privacy and data integrity—and it becomes a challenge for us to know where the CSP is hosting the data center, because the laws are different in different countries with respect to data privacy […], and even if the laws exist, the implementations of the laws are different, and they vary as well."

Provider P4 suggested a simple solution to address the issue of regulations in case of client organizations with a global presence: "The way we handle it together with our clients is that if you have data storage outside Norway, and subsidiaries around the globe, you need to follow the regulations for the mother company." However, by looking at the case of client C1, things do not seem to be that simple. Laws and regulations are very strict because they have already existed before the emergence of cloud services. This was argued by provider P16: "This law was written before CSPs existed. [The law is that the client as a data owner is responsible for ensuring that the data being processed is according to the law; thus, it is not the responsibility of the CSPs]. Companies that adopt cloud services are legally responsible and must ensure that processing personal information is according to the law. […] The conditions today are immature. I think that will change."

Several providers noted that data privacy laws are still applied in the traditional way and have not been adapted to CC services. Regulations are still lagging behind the IT developments, as illustrated by provider P12: "One of the key challenges that I see is that the law-makers aren't up to speed on the new way of delivering data, so regulations will always be, at least, one step behind the technological development." The problem is that governments, through local laws, try to control cloud industry that is borderless by nature. This creates more confusion, as provider P7 pointed out: "When you have the U.S. government looking into your data [. . .] I think that will lead to some restrictions and some rules, but it's going to be difficult to apply those rules as the country borders do not really exist. [. . .] and those are premises for how laws work; if you break a law in Norway, it's by the Norwegian law—if you break the law in England, then it's by the English law—but where is this cyber space law? And if you want to have all the countries agree to something in cyber space, it's not going to happen." This implies the need for international laws; this can be learned from other industries like the financial industry, as provider P1 asserted: "The biggest problem is in policies and laws; CC by its very nature is global! So in order to regulate CC with respect to security and privacy, you need to have international agreement and laws and policies regarding data and privacy."

Second, the issue "Compliance with data privacy Acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services." was ranked high by clients and academics (C = 5, P = 11, and A = 4). Our findings indicate that regulatory compliance restricts clients in their investment in and innovation with CC. Clients from the public sector deal with a lot of sensitive data about the public; thus, they must comply with legal requirements enacted by their government authorities, which restricts their selection of CSPs. In this regard, client C2 stated: "Our organization has a lot of sensitive data […], and there are rules for how […] we are allowed to store our data—we can only buy cloud services from suppliers who can guarantee that these requirements are met." Clients C2 and C11 asserted that non-compliance with regulatory requirements can definitely cause a severe loss of reputation and business.

The interviews indicate that for public sector organizations, laws and regulations play a key role in ensuring the safe use of CC services and, therefore, would influence the investment in the cloud, as pointed out by client C6: "For the public sector, particularly, applying rules for information security is important and would influence the investment in cloud services." Provider P11 had the same opinion that the type of the organization (i.e., public or private) determines the likelihood of the client organization to comply with data privacy Acts: "What works for one vertical industry may not work for another (government, hospitals, banking vs. other verticals that may not have issues and constraints; i.e., regulation and compliance)."

Regulatory compliance is always concerned with the location of the data; client C3, from the healthcare sector, stressed that they wanted to contract cloud services from outside the E.U., but they were not allowed to do that: "There is an opening to utilize cloud services that can document that they are localized in the E.U., but I know, specifically, that we have tried to utilize cloud services, for example, from India, and that has not been allowed—so the laws regarding security of information about citizens are very, very strict." Data protection laws focus on having the data physically located in a certain country or region, which does not fit the borderless nature of the CC model. Provider P5 asserted that regional (i.e., E.U.) and local data privacy laws restrict innovation and cause a segmentation of the market, although data is supposed to move freely across borders: "Cloud services are still showing significant innovation and growth and do

not need any interference from governments. Implementation of standards can force the market to support those standards and restrict innovation. The risk of government intervention may force investors to look at more stable markets. Data needs to be able to flow freely across borders, because cloud services are borderless."

Third, the issue "Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them)." was ranked high by the academics (C = 13, P = 13, A = 1), and it highlights certain transparency problems regarding SLAs, and it appears from our findings that it is the responsibility of the clients to make the SLA clear. For instance, in the case of U.S.-based international CSPs and the Patriot Act issue, clients need to ensure the transparency of SLAs, as C12 (former client and current provider) argued: "If there are underpinning contracts with the provider, they have to make sure that these contracts are foolproof—for instance, I heard about [the Patriot Act] in the U.S., which stipulates that the U.S. government can gain access to [any U.S.-based CSP's datacenters]. However, the trust center of this U.S.-based international CSP will have to obey the U.S. government, but they will transparently involve the customer before providing any access for the U.S. government officials. Thus, as a customer, I have to make sure that a term like that is mentioned in the contract."

Three clients noted that the typical SLA between clients and CSPs defines the acceptable performance level and penalties in case of service interruptions and those current CSPs do not state penalties in their SLAs anymore. This was a concern for many clients who participated in our study, and when we discussed it with several of the providers, they asserted that it is true and it is for a reason. Provider P12 noted: "A lot of vendors really don't operate with SLAs [. . .] they say that you have to trust in our cloud. You share the cloud with 100,000 customers. That is your guarantee that the cloud won't be down, because if it goes down for you, it goes down for 100,000 customers. Then [if we were to pay penalties] we would be out of business. So CSPs don't guarantee 99.9% uptime of the cloud; they just say you have to trust us on this and our track record proves that we have extreme availability." Therefore, the reason for not working with traditional SLAs is that CSPs have a lot of clients, and thus, it would not be affordable for the CSPs to pay penalties for each client, so clients just have to trust their CSP.

Table 4 provides a summary of the findings of the study in answering the research questions raised in the introduction. The most important issues identified and their rankings (i.e., relative importance) from the Delphi study, which belong to three categories (security, strategy and legal and ethical categories). In addition, the important issues that surfaced from the interviews and relate to those three categories are summarized as well. Explanations for “why these issues are important?” are provided from both clients’ and providers’ views. The explanations are provided by the clients and providers whom we had follow-up interviews with. Despite the academics participated in the Delphi stages, they have not been interviewed.

Table 4: Summary of the findings from the Delphi study and follow-up interviews

Category	The most important issues	Clients' view	Providers' view
Security	"The risk of losing control over resources…." Rankings (C = 3, P = 1, A = 2)	-Losing control over data confidentiality, integrity and availability -Losing competitive advantage and reputation -Lack of knowledge about the data location	-The cloud is more secure than in-house -The clients lack competence and skills in security management -Establishing proficient governance audits mitigates public clouds' risks -The security department needs to be involved during the migration to public clouds -Implementing private clouds guarantees security control, but at the expense of scalability and cost effectiveness
	"There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries…." Rankings (C = 6, P = 3, A = 13)	-Concern of having VMs hacked and deleted	-Segregating VMs of different clients from each other is a challenge -Clients need to consider the worst scenarios in mind, and establish trustful relationship
	The political game (emerged from interviews)	-Local CSPs are more secure and compliant with regulations	-Traditional IT providers overstate CC security challenges to discourage clients to move to cloud services -Global CSPs are mature and have best security expertise than local CSPs -Local CSPs often rely on third party providers
	"Many cloud providers claim their compliance with security standards…." Rankings (C = 2, P = 17, A = 9)	-Security needs, including confidentiality, integrity and availability depend on the type of industry in which the client operates and may go beyond security standards	
Strategy	"Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) …." Rankings (C = 7, P = 2, A = 11)	-Service unavailability can interrupt critical operations and cost life -The sensitivity to service levels is associated with the type of industry	-CSPs are vulnerable to lose their trustworthiness due to frequent service unavailability
	"It is important to adopt cloud-service models that have a degree of maturity …." Rankings (C = 8, P = 4, A = 10)	-Criticality of the data determines the choice between CC and on-premise -High volume data generating applications need to be kept on-premise	-Private clouds are more mature for hosting sensitive data
	Maturity of the clients (emerged from interviews)	-Seek agility and overlook maturity of their processes and architecture	-Clients need to have a modular architecture and redesign their business model to realize the benefits from CC services -Investing in CC services should be an integral part of both business and IT strategy
Legal and Ethical	"Data legislation is different and not strong in all countries." Rankings (C = 1, P = 10, A = 3)	-It is often a problem for clients with global presence	-Laws are lagging behind the technological development (strict and exist before CC services) -Using local outdated laws to control borderless CC services is confusing -There is a need for globally agreed laws
	"Compliance with data privacy Acts is mandatory, and it may slow down investing …." Rankings (C = 5, P = 11, A = 4)	-Compliance restricts clients, especially from the public sector, in their investment in CC and selecting CSPs	-The type of the organization (i.e., public or private) determines the demand for compliance, and causes market segmentation
	"Enterprises are faced with weak, undetailed service level agreements (SLAs) from ...." Rankings (C = 13, P = 13, A = 1)	-The concern that current CSPs do not state penalties in their SLAs anymore	-Assuring the SLA's transparency is the responsibility of the client -Not affordable for CSPs to pay penalties for many clients -Clients need to trust the CSPs for their records of high service availability

5. Discussion

The aim of this study has been to explore, identify, and rank the most important issues related to CC adoption, and explain why these issues are important. The interviews supported the findings from the Delphi rankings and provided us with a deeper understanding of the issues. The most important issues belonged to security, strategy, and legal and ethical categories.

First, we found that security risks dominated the rankings, and this was corroborated by the interviews. The risks stem from the fundamental aspects of CC, such as data transfer over the Internet, remote data hosting, and shared virtual resources. Security issues have been extensively researched in the CC and the ASP literature (Subashini & Kavitha 2011; Kern, Kreijger, et al. 2002; Yang & Tate 2012) as well as in the ITO literature in general, with evidence of its impact on ITO decisions and outcomes (Lacity et al. 2010; Lacity et al. 2009).

Viewing CC as an emerging form of ITO, we confirm Schneider and Sunyaev's (2014) finding that the "security risk" is an important determining factor for cloud-sourcing decisions. In addition, we found support for the "Loss of control" factor, which was only weakly supported in Schneider and Sunyaev's (2014). We found that CC entails a significant higher level of risks than traditional ITO, due to the shared virtual resources and data transfer over the Internet, in addition to the remote data hosting. Clients stress that CC security weakness may inhibit the adoption of CC, as it is associated with a number of concerns of losing control over the confidentiality, integrity, and availability of sensitive information and the lack of knowledge as to where the information is stored and replicated.

The most important issue "The risk of losing control over resources . . ." reflects an overarching perspective on the gamut of risks that are or can be associated with CC. Many of the other top ranked issues are related to this issue. The second highest ranked item among providers is "Plans for dealing with incidents . . .", that involves strategies for dealing with incidents, which may occur due to risks implicit in the CC model. Likewise, we found that a number of the highest ranked items can also be seen as manifestations of the same overarching security issue, from either a security, strategic, or legal and ethical perspective.

Our study revealed that most clients invest in CC services as local initiatives, without considering the involvement of IT departments. This tendency to bypass IT departments is one of the most significant security risks (Cloud Security Alliance 2013) and undermines security policies at the business level. We also found that clients generally are not proficient enough in their data security governance, and often they do not even know which questions to ask. This view is supported by Khorshed et al. (2012), as well as participants at the CC Roundtable (Yousif et al. 2014). The providers highlighted this as a matter of educating the clients and having them implement proficient security governance. We therefore conjecture that proficient security governance must be in place before most client companies will trust their data with the CSPs. In large companies, this can be achieved by internal security departments, which would need to build the required competence to assess and mitigate the risks. SMEs may not be able to build such competencies internally. They will have the choice either to trust the CSP or to conduct risk assessments and security audits. Several providers argued that there is a definite need for an independent third party to monitor the cloud services and to provide security audits; this was also advocated by Johan Krebbers, IT architect for Shell's Projects & Technology Business (Yousif et al. 2014). Having third party security audits would then entail significant

extra-costs in most cases. However, as several experts in the provider subpanel noted, most companies have a shallow understanding of the risks to their data with the present systems as well as with cloud solutions. They will need more proficient data security governance procedures anyway.

Providers tended to see the security issue as mainly a lack of security competence and skills among clients. In contrast, several articles and industry reports have documented that CC does imply specific risks on the CSP side, due to shared technology vulnerabilities, unwillingness of CSPs to disclose full details about security practices, and the sheer number of risks and related challenges (Khorshed et al. 2012; Cloud Security Alliance 2013). John Howie, Senior Director of IT Security Services at Microsoft, noted that the threat landscape is evolving, and that they have a threat team that is surveying evolving threats and modifying their controls in a continuous process (Grosse et al. 2010). The Cloud Security Alliance has specified the top seven threats to CC (Cloud Security Alliance 2013): (1) abuse and nefarious use of CC, (2) insecure application programming interfaces, (3) malicious insiders, (4) shared technology vulnerabilities, (5) data loss/leakage, (6) account, service, and traffic hijacking, and (7) unknown risk profile. Tom Edsall, CTO of Cisco's Insieme Business Unit, asserted that the CSP may not comply with the client's standards—and that this constitutes an important problem (Yousif et al. 2014). We, therefore, conjecture that the security threats from the CSP side are still present and our findings also support that CSPs do not provide security level required by the clients. Furthermore, our findings indicate the need for security audits to be conducted on the CSPs to ensure the transparency regarding the provider's security practices and audit reports. Such measures will be important to build trust in the CSP.

The concern over the lack of trust in the multi-tenancy architecture is also reflected in the literature (Owens 2010). Having many customers who share the same IT resources can cause data traffic being hijacked, as multiple tenants sharing the same VM may disrupt the service, unintentionally, causing a denial of service (DoS) attack, which makes the service unavailable (Owens 2010). It is argued that virtualization, which is a core technology for CC, enables the consolidation of physical servers into VMs that are managed by a so-called hypervisor and creates vulnerability that one can traverse from one VM to another client's VM managed by the same hypervisor (Owens 2010). The findings demonstrated that such vulnerabilities caused a lack of trust in the CC model.

Maturity of CSPs is measured in the CC and ITO literature according to the provider's reputation, capabilities in terms of technical and process-related standards, and ability to deliver cloud services as promised (Lacity et al. 2010; Lacity et al. 2009; Schneider & Sunyaev 2014). However, the debate on local CSPs vs. international CSPs is not extensively reflected in the literature. CSPs, especially big international ones, are very concerned about increasing their maturity in the cloud market to compete against local CSPs in securing their cloud services. Some clients, such as C10, think that local CSPs are more likely to store the data within the same country, while this can be an incorrect supposition, as some CSPs might be using third party CSPs to store the data. Furthermore, the skepticism towards global CSPs, who are subject to governments of countries that host the cloud environment, was triggered after the security concerns raised by the Patriot Act, which is debated in the literature (Kshetri & Murugesan 2013).

Interruption of services can be fatal to some clients, and the interviews confirmed that this is an important issue. Service availability is considered critical for core business processes and has to be up 365/24 (Loebbecke et al. 2012). It should, therefore, be considered as an important factor in differentiating CSPs (Schwarz et al. 2009). The literature argues that the cloud market is relatively immature, unlike the traditional ITO market (Schwarz et al. 2009). Events such as CSPs' bankruptcy, service unavailability due to a denial of service (DoS) attack, physical damage to the data center, and government investigations (Jansen & Grance 2011; Venters & Whitley 2012; Subashini & Kavitha 2011) can be very detrimental if they occur.

Second, we saw that strategy issues were prominent in the provider subpanel, and this was corroborated in the interviews. Providers prioritized one significant issue regarding the need for contingency plans for incidents, both in terms of dealing with interruptions of services and migrating to another service provider. Clients, therefore, need to consider contingency plans for worst case scenarios. This requires a certain level of competence and maturity from the client. The ability to create ITO contingency plans is not an explicit factor in Schneider and Sunyaev (2014), but is related to the factors of "Internal IT capabilities" and "strategic vulnerability." Furthermore, the literature recommended evaluating CSPs' financial stability and professional capabilities as well as considering exit plans to guarantee a smooth transition back to the situation before the migration to the cloud (Yao et al. 2010; Altaf & Schuff 2010).

As reported in the interviews, the critical need for service availability depends on the industry, such as healthcare. The literature confirms this and suggests taking a specialized approach to address customers that have very specific needs, such as latency sensitivity (Creeger 2009). This can be achieved by having backup systems to activate services that experience availability problems (Bulchand-Gidumal & Melián-González 2011).

The interviews also indicated the existence of "Snowden effect." Many clients and providers have an increased awareness about the threats that foreign governments pose to the data security, as a direct result of Edward Snowden's revelations. Many of the experts highlighted the need to keep the data outside the U.S., and we may see that CSPs will store data in countries with strong guarantees against governmental intrusion. This factor is lacking in Schneider and Sunyaev's (2014) overview of factors that affect cloud-sourcing decisions, and further research should address this issue from the CSP side.

Client maturity, in terms of the enterprise architecture, and the ability to integrate CC services in an appropriate manner are important prerequisites to be able to realize the potential benefits from CC. Our study revealed that few clients have the appropriate competence and maturity levels. Also, most panelists view cloud technology as still immature and difficult to integrate with the internal IT infrastructure. The interviews revealed that clients often do not have the required maturity levels in terms of standardized processes and modular architecture. In addition, they often do not consider redesigning their business model.

Third, we found that the legal issue of data protection legislation had a high priority for the clients, especially those with a global presence and public sector clients. The literature has reported this issue, “Countries have very different privacy and data protection laws” (Greengard 2012, p.21), and our findings indicate that it is continuing to exist in a more complicated and confusing way for both clients and CSPs. The issue of data protection laws has also been discussed in the literature (Marston et al. 2011; Schneider & Sunyaev 2014) and has been found

to impede the adoption of CC (Iyer & Henderson 2012). Some countries do not have the legislative frameworks for using CC services in the public sector (Shin 2013), and some other countries and regions (i.e., the E.U.) have very strict data privacy laws that should be revisited (Kshetri & Murugesan 2013). Yet, some policy issues need to be reflected in data protection laws (Svantesson & Clarke 2010). Our findings revealed confusion among the CSPs regarding which national law to follow. We found that traditional SLAs are not feasible for CSPs, as they cannot pay penalties to many clients in case of incidents resulting in downtimes. Thus, SLAs in CC are weaker than in traditional ITO, and this contributes to the clients' perceptions of increased security risks and loss of control. Several providers highlighted that clients need to overcome this concern by establishing trustful relationships with CSPs based on their records of high service availability. The SLA aspect is not explicitly covered in Schneider and Sunyaev (2014), but is related to the vendor characteristics "Service capability" and "Trustworthiness", and it, therefore, needs to be further researched in the context of CC.

The regulatory compliance to relevant regulations to CC and legal incentives for green IT (i.e., tax relief) would help businesses to manage their IT and business processes effectively and to gain more market opportunities (Bose & Luo 2011). However, our findings indicate that regulatory compliance restricts businesses in their investment in and innovation with CC. Clients from the public sector deal with a lot of sensitive data about the public; thus, they must comply with legal requirements enacted by their government authorities, which restricts their selection of CSPs. For public organizations, laws and regulations play a key role in ensuring a safe use of CC services, but would slow down the investment in CC services.

In the literature, it is argued that the data protection laws focus on having the data physically located in a certain country or region (Desai 2013; Greengard 2012). This does not fit with the borderless nature of the CC model. Providers in our study noted that privacy laws are lagging behind the development of CC solutions and that there is a need for internationally agreed laws and policies to regulate the adoption of CC. The financial industry has already achieved this, and it will be important to obtain the same goal for a wider adoption of CC. Thus, our findings suggest that law-makers involved in the cloud industry can learn from the financial industry regarding how to create a trustworthy ecosystem and international governance practices. Although the financial industry has achieved a sustainable cloud ecosystem, this happened at the national level (Eaton et al. 2014), but still needs to happen at the global level.

Fourth, the social dimension turned out not to be very prominent in the interviews. However, the issue "People used to old systems will have to change how they work, which is hard and should not be underestimated", was ranked as number six among the providers. It was not ranked among the final top 18 issues among the clients or the academics. We are somewhat puzzled by this result, and speculate that a number of providers may have experienced cloud adoptions being stopped due to client's employees not being ready and motivated to embrace new work processes. This issue concerns the social dimension related to employees and work processes, and should not be underestimated. This issue is also related to the importance of reaching an agreement about a cloud adoption strategy at all levels, which is ranked as number seven by the providers and not ranked by the academics and the clients, and the issue of change management in the migration to the new solution. The transition to a new business model of CC services will require cultural changes in terms of new attitudes and mindsets of the employees. They need to adopt new work routines and unlearn the old ones. Consequently, to ensure efficient migration

processes to CC solutions, clients would benefit from implementing a change management strategy.

6. Conclusion and Implications

As outlined in the introduction, CC has emerged as one of the most influential technologies on a global basis. CC is still in its stage of emergence, and there is still a lack of knowledge and empirical evidence about which issues are most significant for CC adoption decisions. The purpose of this study has been to identify the most important issues related to CC adoption decisions in enterprises.

Figure 2 summarizes the most significant points from the discussion into a framework of CC adoption inhibitors and drivers. The characteristics of CC imply certain risks that companies need to take into account when considering CC adoption. Clients perceive these risks as inhibitors for CC adoption. The experts emphasized security risks, and perceived that security issues constitute the most significant barriers for CC adoption. The specific characteristics of CC lead to a lack of trust in this technology due to the multi-tenancy architecture, remote storing of data, and enterprises fear to lose control over their resources. In addition, CSPs provide weak SLAs to avoid paying penalties to all clients, who share the same virtualized resources in the case of a security breach or data loss incident. Data protection legislation is inhibiting CC adoption, as it constrains clients in trusting CSPs who comply with their specific security needs and regulation, not only the standards. Migration to the cloud and the consequent change can inhibit CC adoption if not planned and managed.

We also conclude that CC adoption should be driven by change management, competence and maturity. Enterprises that consider moving critical business applications to the cloud, should therefore establish solid security governance policies and audits to monitor the CSP's performance. It is important to have detailed plans for dealing with incidents, and private clouds would be preferable in particular critical business environments (e.g. hospitals) to protect sensitive data. Furthermore, it is important for the client to have mature enterprise architecture (EA) and business processes, and understand the shift in the business model, not only in the EA, when moving to the cloud. It is also important to select providers with mature cloud service models.

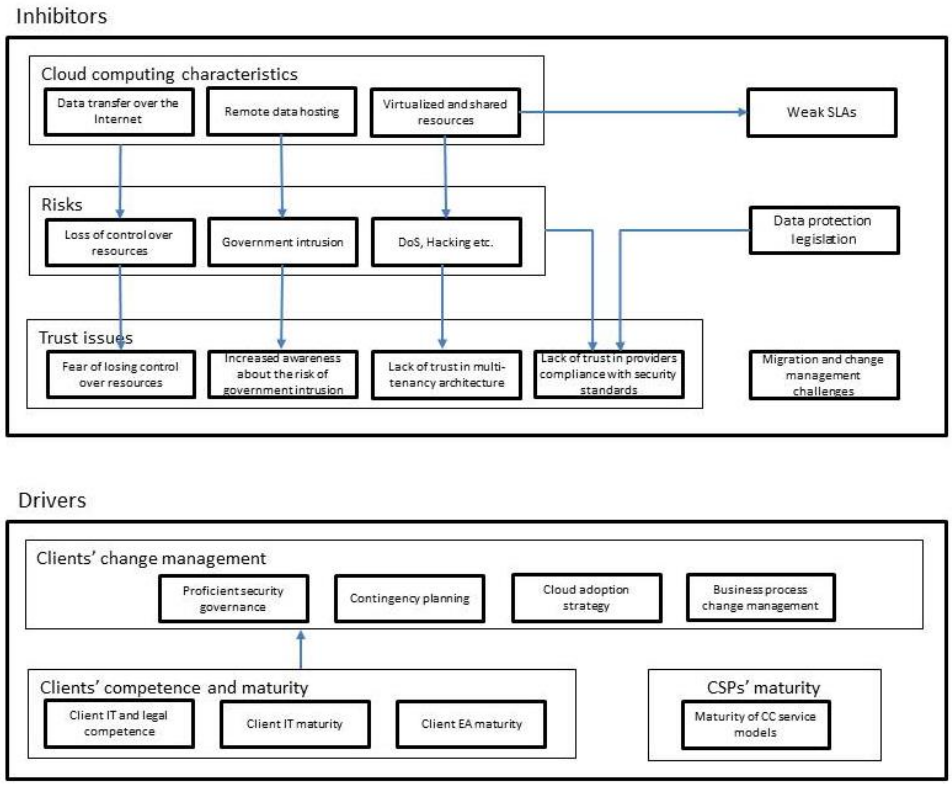


Figure 2: Framework of main inhibitors and drivers for CC adoption

Table 5 provides a list of recommendations that may assist decision-makers in enterprises regarding CC adoption. The recommendations are organized according to the drivers presented in the framework diagram (Figure 2). These recommendations are important implications for practice.

Table 5: Key recommendations for decision-makers regarding CC adoption

Drivers	Recommendations
Client's change management	The client should establish a change management strategy across operational, tactical and strategic levels of the organization to settle any cultural issues. This is important to ensure commitment for CC adoption initiatives. It will require changes in organizing of the IT functions and work routines, and establishing security governance policies.
CC adoption strategy	The client should establish a CC strategy - Decide criticality of business applications and consider cloud readiness of certain business functions, make a prioritized list of which functions and applications that are ready - Consider if the company should move the most critical applications to the cloud - Carefully consider compatibility issues in migration – can the cloud solutions be integrated with existing legacy systems without too much effort and costs? - Be aware of the business context – select private cloud solution if critical environment - Establish risk management practices to evaluate the vulnerability of the firm in case of downtime

Security governance	The client should establish proficient security governance policies as a part of the overall IT governance - Implement data encryption practices and determine the specific security needs - Establish routines for security audits, preferably by hiring an independent third party to assist in understanding the content of and monitoring the SLA, and provide security audits
Contingency planning	The client should have a contingency plan - Develop worst case scenarios and take precautions - Consider lock-in issues and exit plans, establish data transfer options to facilitate change of vendor
Business process change management	The client needs to change business processes to prepare for CC transition - The client needs to be prepared for a shift in the business model which may require radical changes in business processes and a shift in IT responsibilities
Client IT and legal competence	The IT competence of the client is important when taking CC adoption decisions. - IT competence regarding opportunities and constraints for certain solutions - Legal competence: The client should have legal knowledge competencies about data protection legislation and involve external legal expertise if necessary. The client should be aware of potential government intrusion (i.e. Patriot Act)
Client IT maturity	The client should have achieved a certain IT maturity level before adopting CC solutions (especially if the company is well-established with existing IT portfolio). - Enterprise architecture maturity - Maturity in business processes (e.g. business processes are based on best practices) - Maturity in existing IT systems
CSPs' maturity	The client should search for mature CSPs who offer mature CC services - Select a trustable vendor with good reputation in the market - Select CSPs who offer mature CC service models

Finally, the research contributions of this paper are threefold. First, we contribute to the ITO literature on CC. We have highlighted specific strategic issues in CC that have not been highlighted in traditional ITO literature. Second, we provide a discussion of the most important issues as perceived by CC experts and relate these issues to the CC literature. Third, we found that there is a "Snowden effect"—an increased awareness about the threats that foreign governments may pose to the data security, which will influence cloud adoption decisions regarding the location of data storage.

This study is based on the Delphi method as well as interviews of experts in CC. Our sample represents a variety of experts including clients, providers, and academia. The method is not without limitations and has been criticized for its methodological inadequacies (Story et al. 2000). We have been careful to assemble a diverse set of experts and invite only experts with a deep knowledge of the CC topic. A weakness is that the Norwegian context is dominating—but as CC is a borderless technology, we do not believe that it is a serious weakness. We have also used follow-up interviews to further triangulate and provide more depth to our findings.

It is evident that potential adopters of CC technology perceive the adoption decision as very challenging. It is riddled with many issues related to risk management, legal requirements, competence requirements, and IT integration issues. We have highlighted a number of issues that can inform decision-makers who are facing CC investment decisions.

References

Akkermans, H. & Bogerd, P., 2003. The Impact of ERP on Supply Chain Management: Exploratory Findings from a European Delphi Study. *European Journal of Operational Research*, 146(2), pp.284–301. Available at: http://www.sciencedirect.com/science/article/pii/S0377221702005507 [Accessed May 5, 2015].

Altaf, F. & Schuff, D., 2010. Taking a Flexible Approach to ASPs. *Communications of the ACM*, 53(2).

Andriole, S.J., 2012. Seven Indisputable Technology Trends That Will Define 2015. *Communications of the Association for Information Systems*, 30(1). Available at: http://aisel.aisnet.org/cais/vol30/iss1/4 [Accessed March 27, 2015].

Armbrust, B. et al., 2010. A View of Cloud Computing. *Communications of The ACM*, 53(2).

Avrane-Chopard, J. et al., 2014. *Big Business in Small Business : Cloud Services for SMBs*, Available at: http://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/High Tech/PDFs/Big_business_in_small_business_Cloud services_for_SMBs.

Bardhan, I.R. et al., 2010. An Interdisciplinary Perspective on IT Services Management and Service Science. *Journal of Management Information Systems*, 26(4), pp.13–64. Available at: http://mesharpe.metapress.com/openurl.asp?genre=article&id=doi:10.2753/MIS0742-1222260402 [Accessed February 28, 2013].

Bose, R. & Luo, X., 2011. Integrative Framework for Assessing Firms' Potential to Undertake Green IT Initiatives via Virtualization – A Theoretical Perspective. *The Journal of Strategic Information Systems*, 20(1), pp.38–54. Available at: http://www.sciencedirect.com/science/article/pii/S0963868711000047.

Brender, N. & Markov, I., 2013. Risk Perception and Risk Management in Cloud Computing: Results from a Case Study of Swiss Companies. *International Journal of Information Management*, 33(5), pp.726–733. Available at: http://www.sciencedirect.com/science/article/pii/S0268401213000753 [Accessed February 6, 2014].

Bulchand-Gidumal, J. & Melián-González, S., 2011. Maximizing the positive influence of IT for improving organizational performance. *The Journal of Strategic Information Systems*, 20(4), pp.461–478. Available at: http://www.sciencedirect.com/science/article/pii/S0963868711000539 [Accessed September 26, 2014].

Cegielski, C.G. et al., 2012. Adoption of Cloud Computing Technologies in Supply Chains: An Organizational Information Processing Theory Approach. *International Journal of Logistics Management*, 23(2), pp.184–211. Available at: http://www.emeraldinsight.com/10.1108/09574091211265350 [Accessed May 23, 2013].

Chen, P. & Wu, S., 2012. The Impact and Implications of On-Demand Services on Market Structure. *Information Systems Research*, 24(3), pp.1–18. Available at: http://isr.journal.informs.org/content/early/2012/12/20/isre.1120.0451.abstract.

Cloud Security Alliance, 2013. *The Notorious Nine Cloud Computing Top Threats in 2013*, Available at: http://www.cloudsecurityalliance.org.

Creeger, M., 2009. CTO Roundtable: Cloud Computing. *Communications of The ACM*, 52(8), pp.1–7.

Dalkey, N.C., 1972. The Delphi Method: An Experimental Study of Group Opinion. In N. C. Dalkey, ed. *Studies in the quality of life: Delphi and decision-making*. Lexington Books, p. 161.

Day, J. & Bobeva, M., 2005. A Generic Toolkit for the Successful Management of Delphi Studies. *The Electronic Journal of Business Research Methodology*, 3(2), pp.103–116.

Desai, D., 2013. Beyond location: Data Security in the 21st Century. *Communications of the ACM*, 56(1), p.34. Available at: http://dl.acm.org/citation.cfm?doid=2398356.2398368 [Accessed March 7, 2013].

Dibbern, J. et al., 2004. Information Systems Outsourcing: A Survey and Analysis of the Literature. *ACM SIGMIS Database*, 35(4), pp.6–102. Available at: http://dl.acm.org/citation.cfm?id=1035233.1035236 [Accessed February 25, 2015].

Dorey, P. & Leite, A., 2011. Commentary: Cloud Computing–A Security Problem or Solution? *Information Security Technical Report*, 16(3), pp.89–96. Available at: http://www.sciencedirect.com/science/article/pii/S1363412711000495 [Accessed May 4, 2015].

Eaton, B. et al., 2014. Achieving Payoffs from an Industry Cloud Ecosystem at BankID. *MIS Quarterly Executive*, 13(4), pp.223–235.

Fielt, E. et al., 2013. Editorial: Service Management and Engineering in Information Systems Research. *The Journal of Strategic Information Systems*, 22(1), pp.46–50. Available at: http://dl.acm.org/citation.cfm?id=2450855 [Accessed May 5, 2015].

Franklin, K. & Hart, J., 2007. Idea Generation and Exploration: Benefits and Limitations of the Policy Delphi Research Method. *Innovative Higher Education*, 31(4), pp.237–246. Available at: http://link.springer.com/article/10.1007/s10755-006-9022-8 [Accessed May 5, 2015].

Galliers, R.D. et al., 2012. Strategic information systems: Reflections and prospectives. *The Journal of Strategic Information Systems*, 21(2), pp.85–90. Available at: http://www.sciencedirect.com/science/article/pii/S096386871200025X [Accessed April 1, 2014].

Garg, S.K., Versteeg, S. & Buyya, R., 2013. A Framework for Ranking of Cloud Computing Services. *Future Generation Computer Systems*, 29(4), pp.1012–1023. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167739X12001422 [Accessed March 3, 2013].

Garrison, G., Kim, S. & Wakefield, R.L., 2012. Success Factors for Deploying Cloud Computing. *Communications of the ACM*, 55(9), pp.62–68.

Greengard, S., 2012. On the Digital Trail. *Communications of the ACM*, 55(11), p.19. Available at: http://dl.acm.org/citation.cfm?doid=2366316.2366323 [Accessed March 6, 2013].

Grosse, E. et al., 2010. Cloud Computing Roundtable. *IEEE Security & Privacy Magazine*, 8(6), pp.17–23. Available at: http://www.computer.org/csdl/mags/sp/2010/06/msp2010060017.html [Accessed May 4, 2015].

Gupta, P., Seetharaman, A. & Raj, J.R., 2013. The Usage and Adoption of Cloud Computing by Small and Medium Businesses. *International Journal of Information Management*, 33(5), pp.861–874. Available at: http://linkinghub.elsevier.com/retrieve/pii/S026840121300087X [Accessed August 24, 2013].

Hashizume, K. et al., 2013. An Analysis of Security Issues for Cloud Computing. *Journal of Internet Services and Applications*, 4(1), p.5. Available at: http://www.jisajournal.com/content/4/1/5 [Accessed April 9, 2015].

Hsu, C. & Sandford, B.A., 2007. The Delphi Technique: Making Sense of Consensus. *Practical Assessment, Research & Evaluation*, 12(10), pp.1–8.

Iden, J., Tessem, B. & Päivärinta, T., 2011. Problems in the interplay of development and IT operations in system development projects: A Delphi study of Norwegian IT experts. *Information and Software Technology*, 53(4), pp.394–406. Available at: http://www.sciencedirect.com/science/article/pii/S095058491000217X [Accessed March 31, 2014].

Iyer, B. & Henderson, J.C., 2012. Business Value from Clouds: Learning from Users. *MIS Quarterly Executive*, 11(1), pp.51–60.

Iyer, B. & Henderson, J.C., 2010. Preparing for The Future: Understanding The Seven Capabilities of Cloud Computing. *MIS Quarterly Executive*, 9(2), pp.117–131.

Jansen, W. & Grance, T., 2011. *Guidelines on Security and Privacy in Public Cloud Computing*, Available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Kappelman, L. & McLeon, E., 2013. Key Issues of IT Organizations and Their Leadership: The 2013 SIM IT Trends Study. *MIS Quarterly Executive*, 12, pp.227–240. Available at: http://www.researchgate.net/publication/263618863_Key_Issues_of_IT_Organizations_and_Their_Leadership_The_2013_SIM_IT_Trends_Study [Accessed May 4, 2015].

Keil, M., Lee, H. & Deng, T., 2013. Understanding the Most Critical Skills for Managing IT Projects: A Delphi Study of IT Project Managers. *Information & Management*, 50(7), pp.398–414. Available at: http://www.sciencedirect.com/science/article/pii/S0378720613000475 [Accessed May 5, 2015].

Kendall, M. & Gibbons, J., 1990. *Correlation Methods*, Available at: https://scholar.google.no/scholar?q=kendall+and+gibbons&btnG=&hl=en&as_sdt=0%2C5#4 [Accessed May 5, 2015].

Kern, T., Kreijger, J. & Willcocks, L., 2002. Exploring ASP as Sourcing Strategy: Theoretical Perspectives, Propositions for Practice. *The Journal of Strategic Information Systems*, 11(2), pp.153–177. Available at: http://www.sciencedirect.com/science/article/pii/S0963868702000045 [Accessed September 26, 2014].

Kern, T., Lacity, M.C. & Willcocks, L.P., 2002. An Overview of Netsourcing. In *Netsourcing: Renting Business Applications and Services Over a Network*. New Jersey: Financial Times (Prentice Hall), p. 368.

Khorshed, M., Ali, A. & Wasimi, S., 2012. A Survey on Gaps, Threat Remediation Challenges and Some Thoughts for Proactive Attack Detection in Cloud Computing. *Future Generation computer systems*, 28(6), pp.833–851. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X12000180 [Accessed May 5, 2015].

Kshetri, N., 2013. Privacy and Security Issues in Cloud Computing: The Role of Institutions and Institutional Evolution. *Telecommunications Policy*, 37(4-5), pp.372–386. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0308596112000717 [Accessed March 4, 2013].

Kshetri, N. & Murugesan, S., 2013. Cloud Computing and EU Data Privacy Regulations. *Computer*, 46(3), pp.86–89. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6489955.

Lacity, M.C. et al., 2010. A Review of the IT Outsourcing Empirical Literature and Future Research Directions. *Journal of Information Technology*, 25(4), pp.395–433. Available at: http://www.palgrave-journals.com/doifinder/10.1057/jit.2010.21 [Accessed December 24, 2014].

Lacity, M.C., Khan, S.A. & Willcocks, L.P., 2009. A Review of the IT Outsourcing Literature: Insights for Practice. *The Journal of Strategic Information Systems*, 18(3), pp.130–146. Available at: http://www.sciencedirect.com/science/article/pii/S0963868709000195 [Accessed July 13, 2014].

Lacity, M.C. & Reynolds, P., 2014. Cloud Services Practices for Small and Medium-Sized Enterprises. *MIS Quarterly Executive*, 13(1), pp.31–44.

Loebbecke, C., Thomas, B. & Ullrich, T., 2012. Assessing Cloud Readiness at Continental AG. *MIS Quarterly Executive*, 11(1), pp.11–22.

Luftman, J. et al., 2012. Key Information Technology and Management Issues 2011–2012: An International Study. *Journal of Information Technology*, 27(3), pp.198–212. Available at: http://www.palgrave-journals.com/jit/journal/v27/n3/abs/jit201214a.html [Accessed February 2, 2015].

Malladi, S. & Krishnan, M.S., 2012. Cloud Computing Adoption and its Implications for CIO Strategic Focus – An Empirical Analysis. In *Proceedings of 33rd International Conference on Information Systems (ICIS 2012)*. pp. 1–19.

Marston, S. et al., 2011. Cloud computing — The Business Perspective. *Decision Support Systems*, 51(1), pp.176–189. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923610002393 [Accessed February 27, 2013].

Mcgeogh, B.T. & Donnellan, B., 2013. Factors That Affect the Adoption of Cloud Computing for an Enterprise : A Case Study of Cloud Adoption Within Intel Corporation. In *Proceedings of the 21st European Conference on Information Systems*. pp. 1–13.

Mell, P. & Grance, T., 2011. The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. , pp.1–7. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Muhic, M. & Johansson, B., 2014. Cloud Sourcing – Next Generation Outsourcing? *Procedia Technology*, 16, pp.553–561. Available at: http://www.sciencedirect.com/science/article/pii/S2212017314002308 [Accessed November 15, 2014].

Myers, M.D. & Newman, M., 2007. The Qualitative Interview in IS Research: Examining the Craft. *Information and Organization*, 17(1), pp.2–26. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1471772706000352 [Accessed March 23, 2014].

Okoli, C. & Pawlowski, S.D., 2004. The Delphi Method as a Research Tool: An Example, Design Considerations and Applications. *Information & Management*, 42(1), pp.15–29.

Owens, D., 2010. Securing Elasticity in The Cloud. *Communications of The ACM*, 53(8), pp.1–7. Available at: http://portal.acm.org/citation.cfm?doid=1794514.1794516.

Schmidt, R. et al., 2001. Identifying Software Project Risks: An International Delphi Study. *Journal of Management Information Systems*, 17(4), pp.5–36. Available at: http://portal.acm.org/citation.cfm?id=1289670.

Schmidt, R.C., 1997. Managing Delphi Surveys Using Nonparametric Statistical Techniques. *Decision Sciences*, 28(3), pp.763–774. Available at: http://doi.wiley.com/10.1111/j.1540-5915.1997.tb01330.x [Accessed March 23, 2014].

Schneider, S. & Sunyaev, A., 2014. Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. *Journal of Information Technology*, pp.1–31. Available at: http://www.palgrave-journals.com/doifinder/10.1057/jit.2014.25 [Accessed December 10, 2014].

Schwarz, A. et al., 2009. A Conjoint Approach to Understanding IT Application Services Outsourcing. *Journal of the Association for Information Systems*, 10(10), pp.748–781.

Shin, D.-H., 2013. User Centric Cloud Service Model in Public Sectors: Policy Implications of Cloud Services. *Government Information Quarterly*, 30(2), pp.194–203. Available at: http://www.sciencedirect.com/science/article/pii/S0740624X13000099 [Accessed July 30, 2014].

Stieninger, M. et al., 2014. Impacts on the Organizational Adoption of Cloud Computing: A Reconceptualization of Influencing Factors. *Procedia Technology*, 16, pp.85–93. Available at: http://www.sciencedirect.com/science/article/pii/S2212017314002989 [Accessed November 12, 2014].

Story, V. et al., 2000. Methodological and Practical Implications of the Delphi Technique in Marketing Decision-Making: A Re-Assessment. *The Marketing Review*, 1(4), pp.487–504. Available at: http://www.ingentaconnect.com/content/westburn/tmr/2000/00000001/00000004/art00006 [Accessed May 5, 2015].

Su, N. et al., 2009. Shared Services Transformation : Conceptualization and Valuation from the Perspective of Real Options. *Decision Sciences*, 40(3), pp.381–402.

Subashini, S. & Kavitha, V., 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*. Available at: http://www.sciencedirect.com/science/article/pii/S1084804510001281 [Accessed May 5, 2015].

Susarla, A., Barua, A. & Whinston, A., 2003. Understanding the Service Component of Application Service Provision: An Empirical Analysis of Satisfaction with ASP Services. *MIS Quarterly*, 27(1), pp.91–123.

Svantesson, D. & Clarke, R., 2010. Privacy and Consumer Risks in Cloud Computing. *Computer Law & Security Review*, 26(4), pp.391–397. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0267364910000828 [Accessed March 2, 2013].

Venters, W. & Whitley, E. a, 2012. A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology*, 27(3), pp.179–197. Available at: http://www.palgrave-journals.com/doifinder/10.1057/jit.2012.17 [Accessed March 4, 2013].

Ward, J.M., 2012. Information Systems Strategy: Quo Vadis? *The Journal of Strategic Information Systems*, 21(2), pp.165–171. Available at: http://www.sciencedirect.com/science/article/pii/S0963868712000182 [Accessed April 1, 2014].

Yang, H. & Tate, M., 2012. A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 31(1), pp.35–60.

Yao, Y., Watson, E. & Khan, B. k., 2010. Application Service Providers: Market and Adoption Decisions. *Communications of the ACM*, 53(7), pp.113–117.

Yousif, M. et al., 2014. Cloud Computing Roundtable. *IEEE Cloud Computing*, 1(1), pp.40–49.

Zissis, D. & Lekkas, D., 2012. Addressing Cloud Computing Security Issues. *Future Generation computer systems*, 28(3), pp.583–592. Available at: http://www.sciencedirect.com/science/article/pii/S0167739X10002554 [Accessed May 4, 2015].

Appendix:

Table A: List of 55 issues identified by the experts and grouped into 10 main categories

Category	Issues
Security (14 issues)	• Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.
	• The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.
	• The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.
	• It is unclear who owns the data
	• Malicious insiders (i.e., cloud provider's employees) may access the cloud servers and steal confidential data of the cloud users.
	• One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.
	• Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.
	• There may be insufficient and inconsistent data encryption policies and practices.
	• There are real security risks related to data theft, hacking, virus attacks, and data corruption. Specifically, if the hypervisor layer becomes compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding these issues.
	• There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.
	• There is concern about making the data lifecycle secure in all its phases (i.e., create, store, use, share, archive, and destroy). An insecure data lifecycle may lead to data leakage. Regarding data deletion, if the provider does not provide proof that its data-wiping technique prevents data recovery, this will put customer data (i.e., financial data, employee records, or medical records) at risk, causing confidentiality problems, thus affecting the enterprise's reputation.
	• Multiple tenants may disrupt services unintentionally, causing a denial of service (DoS) attack that makes services unavailable, which leads to losing customers.
	• Enterprises in a certain geographic location trust in or are forced by the government to deal with cloud providers within their area, whether they provide the best service or not. On the other hand, these providers might be using third-party providers to store the data.
	• The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.
Availability (1 issue)	• There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity.
Migration (3 issues)	• Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.
	• The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.
	• There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.
Business (9 issues)	• If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.

Category	Issues
	• Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.
	• The transition from capital expenditure to operational expenditure reduces operational margins but increases operational risks and could lead to a less predictable cost level.
	• Cloud solutions are difficult to sell because they are not supported by traditional sales models.
	• Cloud computing offers financial benefits and very well-articulated services but results in a higher total cost of ownership (TCO).
	• Budget constraints may lead to delays in implementing current visions. It has to be clear to the top management how much money can be saved in the future when spending so much at once.
	• There is fear of losing business and long-term brand recognition.
	• The slow development of suitable standards causes the lack of technological innovation within the cloud industry.
	• A significant amount of negative marketing exists in cloud services.
Legal and ethical (7 issues)	• Data protection legislation is different and not strong in all countries.
	• Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.
	• It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects.
	• Standardized cloud-process models do not support customization, and organizations may have to change their processes and practices to maximize the benefits.
	• Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).
	• There is no standard service level agreement (SLA) for cloud computing delivery methods due to unsolved security and environmental (such as supplier dependency) issues, which will lead to unclear segregation of duties between the cloud provider and the consumer (due to the lack of legal precedents) regarding responsibilities for personal and sensitive business data at the level of the service models, IaaS, PaaS, and SaaS). This raises potential security vulnerabilities.
	• It is hard for small clients to modify the standard agreements of major international cloud providers.
Culture (2 issues)	• People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.
	• Some key people in the organization are powerful, and management may fear confronting them with change if they strongly oppose it.
Awareness (4 issues)	• The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.
	• There is reluctance to adopt a cloud service with less functionality or reduced user experience (efficiency and flexibility) than that of traditional solutions.
	• The consumer's lack of security awareness results in misuse of the cloud environment and misconfiguration of the cloud-environment layers.
	• There is a lack of analysis and sales activities as some vendors deliver IaaS as though it should be a pure public cloud. However, when clients more closely examine how vendors deliver their services, these do not fulfill customer expectations (some services are not automatically created, which cost effort and money to create) and turn out to be more like traditional outsourcing that is packed as a cloud service, sales wise.
Impact (7 issues)	• Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.
	• User support is a critical component in building trust between business operations and IT services.
	• Organizations may fail to modify their business processes to leverage the effect of cloud computing agility on business models.

Category	Issues
	• There is concern about whether the transition to the cloud disturbs current IT and business operations.
	• Cloud computing offers an opportunity for reorganizing the IT department (laying off dedicated staff).
	• Maintaining an old organizational chart will lead to gaps in understanding new requirements from all involved teams.
	• The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.
IT Governance (1 issue)	• There is a lack of IT governance tools, policies, and best practices particular to cloud-service management.
Strategy (7 issues)	• It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it *must* be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.
	• The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.
	• There is a huge variance in the demands for each organization/department/employee. Thus, the chosen model(s) have to serve all needs in the most efficient way compared to the traditional methods.
	• In many cases, the adoption is more "random," and the benefits disappear because key considerations are overlooked (in terms of what organizations actually want, what they expect, why they want to adopt the cloud, what can be implemented in the cloud, and how to transition).
	• Each organization is required to describe its enterprise architecture in detail to easily contract the correct cloud services for the "to-be" architecture.
	• Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.
	• It is important to evaluate the provider (in terms of experience with the industry, ability to provide advice on "cloud orchestration," operational stability, and long-term commitment) and ensure that prices are comparable across different vendors.

Table B: Ranking results from first ranking round, ranking of 33 issues.

CR=Combined Ranked, MR=Mean Rank, R=Rank, C=Client panel, P=Provider panel, A=Academic panel.

Issues (N=33)	**CR (MR)**	**CR (R)**	**C(MR) N=8**	**C(R)**	**P(MR) (N=14)**	**P(R)**	**A(MR) N=5**	**A(R)**
Security (The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them).	11,07	1	11,5	3	11,29	1	9,8	2
Strategy (Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations).	12,15	2	12,88	5	11,29	2	13,4	11
Legal and Ethical (Data protection legislation is different and not strong in all countries).	12,81	3	8,88	1	15,93	10	10,4	3
Security (There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage).	13	4	13,38	6	11,86	3	15,6	13
Security (Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for).	14,19	5	9,88	2	17,07	17	13	9
Legal and Ethical (Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services).	14,33	6	12,88	4	16,29	12	11,2	4
Strategy (It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it must be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud).	14,59	7	15,25	12	15	5	12,4	8
Legal and Ethical (Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they	14,78	8	16,13	16	16,29	13	8,4	1

store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them)).								
IT Governance (There is a lack of IT governance tools, policies, and best practices particular to cloud-service management).	15,41	9	15,5	15	15,07	7	16,2	17
Legal and Ethical (It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects).	16,48	10	16,38	17	15,07	6	20,6	24
Security (The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational).	16,52	11	16,88	19	16,5	14	16	15
Migration (The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity).	16,96	12	14	7	16,14	11	24	30
Impact (Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds).	17,19	13	15,5	14	18,5	26	16,2	16
Availability (There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity).	17,33	14	17,38	20	17,5	19	16,8	18
Security (One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met).	17,37	15	15,5	13	18,14	22	18,2	22

Impact (The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions).	17,41	16	14,75	10	20,5	31	13	10
Security (The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises).	17,48	17	14,13	8	17,86	21	21,8	26
Impact (There is concern about whether the transition to the cloud disturbs current IT and business operations).	17,52	18	16,5	18	20,14	28	11,8	6
Security (Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information).	17,74	19	18,88	23	17,07	16	17,8	20
Strategy (The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative).	17,81	20	20,5	26	14,71	4	22,2	29
Business (If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy).	17,96	21	15,13	11	18,14	23	22	28
Migration (There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations).	18,07	22	22,88	31	15,36	8	18	21
Awareness (The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value).	18,3	23	21,5	29	17,43	18	15,6	14
Culture (People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be	18,44	24	20,25	24	15,43	9	24	31

underestimated).								
Impact (Organizations may fail to modify their business processes to leverage the effect of cloud computing agility on business models).	18,74	25	20,5	25	18,29	25	17,2	19
Security (There are real security risks related to data theft, hacking, virus attacks, and data corruption. Specifically, if the hypervisor layer becomes compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding these issues).	18,93	26	17,63	21	18,79	27	21,4	25
Security (It is unclear who owns the data).	19,22	27	25,88	33	18,21	24	11,4	5
Security (There may be insufficient and inconsistent data encryption policies and practices).	19,3	28	14,63	9	21	33	22	27
Legal and Ethical (It is hard for small clients to modify the standard agreements of major international cloud providers).	19,33	29	21	28	20,86	32	12,4	7
Migration (Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud).	19,48	30	21	27	20,36	30	14,6	12
Security (Enterprises in a certain geographic location trust in or are forced by the government to deal with cloud providers within their area, whether they provide the best service or not. On the other hand, these providers might be using third-party providers to store the data.	19,52	31	17,88	22	20,36	29	19,8	23
Business (Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate).	20,7	32	21,88	30	17	15	29,2	33
Impact (User support is a critical component in building trust between business operations and IT services).	20,85	33	24,25	32	17,57	20	24,6	32
Kendall *W*	**0,064**		**0,173**		**0,069**		**0,270**	
Sign	**0,006**		**0,072**		**0,533**		**0,089**	

Appendix B: Documentation of Data Collection and Data Analysis

1	Brainstorming Survey
2	Narrowing-Down Survey
3	Ranking Round One Survey
4	Ranking Round Two Survey
5	Sample Key Interview Questions
6	Delphi Study Report to Experts
7	Examples of Data Analysis

Cloud Computing Delphi Study
Research Project at University of Agder, Department of Information Systems

Enterprise Research Team:

PhD Candidate: Rania El-Gazzar
Associate Professor: Eli Hustad
Professor: Dag Håkon Olsen

Objectives of the Pilot study:

The basic objective of the pilot study is twofold:

1. To make sure the questionnaire is not ambiguous and the given instructions are sufficient (i.e., comments for improvement and feedback are welcomed).
2. To brainstorm about the current important issues that could concern enterprises when adopting cloud services.
   ⇒ Note that the term adoption refers to the process from the enterprise first decides to adopt cloud service to the implementation and becoming a routinized practice.

Participant Information:

We would appreciate if you kindly provide the information needed by the following table; this information will be used for classification purposes and will be anonymized during the Delphi rounds:

Name:	
Position:	
Current Employment	**Put x letter inside the brackets** ( ) Academia ( ) Client/User ( ) Cloud Provider ( ) Vendor ( ) Consultancy Other (please specify) ----------
Company Name:	
Years of experience in IT/IS:	
Years of experience in cloud computing:	
Country:	

Questionnaire 1:

Start Date: 10/2/2014 **End Date: 16/2/2014**

Kindly answer the following question and send this file with the answer, before the End Date specified above, to this e-mail: rania.f.el-gazzar@uia.no

Q: What are the issues that enterprises are confronted with when adopting cloud computing services?

- Please provide the answer to this question in the dedicated table below with regard to the following instructions:
  - Provide at least 6 issues in the "Issues" column. If you have more issues to elaborate on, please feel free to use more rows in the table below.
  - State a reason why each issue is important in the "Why important" column.
  - Describe briefly the consequences caused by each issue in the "Consequences" column.
  - If there is an important note, advices, or quotes from experience regarding any issue, please provide it in the "Comments" column.

Issues	**Why important**	**Consequences**	**Comments**

Cloud Computing Delphi Study (Round II: Narrowing Down)

Research Project at University of Agder, Department of Information Systems

Enterprise Research Team:
PhD Candidate: Rania El-Gazzar
Associate Professor: Eli Hustad
Professor: Dag Håkon Olsen

Note: The Survey Consist of 2 pages: Page 1 (Concerning Issues) and Page 2 (Motivating Issues)

University of Agder, Kristiansand, Norway

Concerning Issues

There are 10 categories containing 55 Issues. Kindly select between 10 (as a minimum) and 20 (as a maximum) of the 55 issues.

1. **Business**

Mark only one oval per row.

	Important
• Fear of losing business and long term brand recognition	
• Cloud solutions are difficult to sell because they are not supported by traditional sales models	
• Financial Benefits and very well-articulated services but higher Total Cost of Ownership (TCO)	
• Budget constraints may lead to a delays in implementing current visions and it has to be clear for the top management how much money can be saved in the future when spending so much at once	
• The transition from CapEx to OpEx reduces operational margins but increases operational risks and could lead to a less predictable cost level	
• Little investment costs when transferring to a cloud solution but must expect a higher monthly rate	
• If the cost of using Cloud services is not lower than On-premise, it is difficult to get the cloud strategy supported by the management	
• The slow development of rightful standards caused lack of technological innovation within cloud industry	
• Significant amount of negative marketing about cloud services	

2. **Migration**

Mark only one oval per row.

	Important
• Each team/department/Organization adopting their own concept of a cloud and it becomes difficult to migrate all the clouds into one big cloud	
• Lock-in concern about taking back the data and software from one cloud vendor to another, if the service is not satisfactory, without affecting business operations	
• Lack of uniform support models makes it complex to integrate cloud solutions with the legacy on-premise IT infrastructure as well as data from different sources which costs effort and time and may affect applications availability and data integrity	

3. **Security**

Mark only one oval per row.

	Important
• Malicious insiders (i.e., cloud provider's employees) may access the cloud servers and steal confidential data of the cloud user	
• Using public cloud services (Bring Your Own Cloud – BYOC) for project collaboration may threaten employees' personal data and business confidential data and makes it difficult to maintain and control a security policy for access and distribution of corporate information	
• The risk of moving enterprise's customer data to the cloud leaves enterprises hesitant either to stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises	
• Insufficient and inconsistent data encryption policies and practices	
• It is unclear who owns the data	
• The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than public clouds. However, risks are not absolute and most of them can be addressed but not all of them	
• Real security risks related to data theft, hacking, virus attacks, data corruption. Especially, if the hypervisor layer got compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding that	
• The concern about making the data lifecycle secure in all its phases (i.e., create, store, use, share, archive, and destroy). Insecure data lifecycle may lead to data leakage. Regarding data deletion, if the provider didn't provide proof that their data wiping technique prevents its recovery, this will put customer data (i.e., financial data, employee records, or medical records) at risk causing confidentiality problems, thus, affecting enterprise's reputation	
• One provider's SaaS application can be based on another	

provider's PaaS solution that runs on other provider's IaaS offering, which adds another lever of security risks and becomes difficult to trace whether or not legislation and internal security policies are met	
• The security department involvement is important at every step of the migration, from the requirements gathering, the technical implementation and till the support cycle is in production and running	
• Multiple tenants disrupt services unintentionally causing Denial of Service (DoS) attack that makes service unavailable, which leads to losing customers	
• Many cloud providers claim that they are compliant with security standards, but enterprises want to make sure that this is of relevance to the kind of security they are looking for	
• Enterprises in a certain geographical location trust in, or forced by the government to deal with, cloud providers within their area whether they provide the best service or not. While these providers might be using 3rd party providers to store the data	
• Lack of trust in the cloud's multi-tenancy architecture and the governments of countries where data is stored. Thus, data need to be encrypted to make it hard to use customer data in case of data leakage	

4. **Legal & ethical**

Mark only one oval per row.

	Important
• There is no standard SLA for cloud computing delivery method due to unsolved security and environmental (such as supplier dependency) issues, which will lead to unclear segregation of duties between cloud provider and the consumer (due to lack of law suits regarding responsibilities for personal and business sensitive data at the level of service models IaaS, PaaS, and SaaS). This raises potential security vulnerabilities	
• Enterprises are faced with weak undetailed Service Level Agreements (SLAs) from providers (e.g., providers may not be transparent about where and how do they store the data and the acknowledgement of security incidents whenever happen and how the cloud provider deals with it)	
• It is hard for small clients to modify the standard agreements of major international cloud providers	
• Compliance with data privacy Acts is mandatory and it may slow investing in and exploiting the full benefits of cloud services	
• Data protection legislations are different and not strong in all countries	
• Laws and standards are difficult for companies to get an overview of them and make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects	
• Standardized cloud process models do not support customization and you may have to change your processes and practices to get the most out of its benefits	

5. **Culture**

Mark only one oval per row.

	Important
• People being used to old systems will have to change how they work (more automation, less paperwork, new routines etc), and this is hard for many people and should not be underestimated	
• Some key people in the organization are very strong and Management could fear to confront them with change if they are heavily against it	

6. **Awareness**

Mark only one oval per row.

	Important
• Lack of analysis and sales activities as some vendors deliver IaaS as it should be a pure public cloud, but when clients look closer on how the vendors deliver their services it does not fulfill what they expect (some services are not automatically created which cost effort and money to create) and it turns to be more like traditional outsourcing which is packed as a cloud service sale wise	
• Lack of security awareness that results in misuse of cloud environment as a consumer and misconfiguration of cloud environment layers	
• The meaning of cloud, the difference between it and on-premise, and the consequence of using it is not clear for the users (including managers) which may weaken its value	
• Reluctance to adopt a cloud service with less functionality or reduced user experience (efficiency and flexibility) than a traditional solutions	

7. **IT Governance**

Mark only one oval per row.

	Important
• Lack of IT governance tools, policies, and best practices particular to cloud service management	

8. **Availability**

Mark only one oval per row.

	Important
• The concern about assuring appropriate connectivity for enterprises and their customers avoid negative impact on productivity	

9. **Strategy**

Mark only one oval per row.

	Important
• There is a huge variance in the demands for each organization/department/employee . Thus, the chosen model(s) has to serve all the needs in the most efficient way as compared to the traditional methods	
• The importance of evaluating the provider (in terms of experience with the industry and able to provide advice on “cloud orchestration”, provider’s operational stability and long term commitment) and ensuring that prices are comparable across different vendors	
• Plans for dealing with incidents (downtime, provider goes bankrupt, and the data center is destroyed) should be in place to keep business critical operations running	
• Each organization is required to make a detailed description of its enterprise architecture to easily contract the correct cloud services for the TO-BE architecture	
• It is important to adopt cloud service models have a degree of maturity that the sensitive data and functions can be implemented in private cloud, otherwise, MUST be kept on-premise. While non-sensitive data and functions can be outsourced to the cloud	
• The adoption, in many case, is more “random” and the benefits disappear because key considerations were overlooked (in terms of what you actually want, what you expect, why you want to adopt the cloud, what can be implemented in the cloud, and how to transition)	
• Lack of reaching an agreement about cloud adoption strategy at all levels can kill of the best-intended initiative	

10. **Impact**

Mark only one oval per row.

	Important
• Sticking to an old organizational chart will lead to gaps in understanding new requirements from all involved teams	
• Implementing cloud services in your organization requires a different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers) which can be expensive and time-consuming, especially, in implementing private clouds	
• Failure to modify business processes in order to leverage the effect of cloud computing agility on the business model	
• User support is a critical component in building trust between business operations and IT services	
• An opportunity for rationalization in the IT department (laying off dedicated staff)	
• The company is dependent on external routines and competence and if something happens the enterprise cannot solve the issue themselves and the enterprise will be unable to perform its normal duties	
• The concern that the transition to the cloud doesn't disturb current IT and Business Operations	

Motivating Issues

There are 9 categories containing 12 issues. Kindly select at least six issues.

11. **Cloud is more secure than on-premise**

Mark only one oval per row.

	Important
• Security often is more at risk in companies where systems are local than where systems are cloud-based (security in cloud systems is of higher competence than in an average local stored company)	

12. **Professionalism**

Mark only one oval per row.

	Important
• A solution for small organizations that do not have the capacity and/or competencies to operate/maintain themselves	

13. **Collaboration**

Mark only one oval per row.

	Important
• Collaboration in a business context is supported by cloud based services	

14. **"Bring your own cloud" (BYOC)**

Mark only one oval per row.

	Important
• Employees may install public cloud services such as Dropbox and iCloud on their corporate desktops and mobile devices without any clear adoption decision	

15. **Flexibility**

Mark only one oval per row.

	Important
• Access to services from anywhere and from/across different platforms without putting too much investment prior to the needs	

16. **Economic**

Mark only one oval per row.

	Important
• Helps the company grow its regular income; it is good with sable income over time which makes it easier to estimate budgets	
• Low up-front investments as well as predictable and scalable operation expenses	
• Cloud services increase efficiency and decrease costs	

17. **Efficiency**

Mark only one oval per row.

	Important
• Clients using cloud services can focus on core business activities rather than on IT operations	

18. **Integration**

Mark only one oval per row.

	Important
• Most cloud solutions today utilize web services which are a new technology that support integrations	

19. **Performance**

Mark only one oval per row.

	Important
• Most cloud solutions have nearly no «downtime» because IT professionals provide surveillance over servers days and nights to ensure service availability	
• Stable operations and effective running up time	

Cloud Computing Delphi Study (Round III: Ranking)

Ranking Concerns

University of Agder, Kristiansand, Norway
Enterprise Research Team:
PhD Candidate: Rania El-Gazzar
Associate Professor: Eli Hustad
Professor: Dag Håkon Olsen

Instructions:
The purpose of this survey is to rank the concerns that are chosen in the second round. This survey consists of a list of 33 concerns to rank with a space for comments or justifications on the rankings at the end of the survey.

1. Kindly rank the following concerns from 1 (highest priority) to 33 (lowest priority) by simply dragging each item upward or downward and the ranking will adjust automatically.

	• Using public cloud services (Bring Your Own Cloud – BYOC) for project collaboration may threaten employees' personal data and business confidential data and makes it difficult to maintain and control a security policy for access and distribution of corporate information
	• The risk of moving enterprise's customer data to the cloud leaves enterprises hesitant either to stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises
	• The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than public clouds. However, risks are not absolute and most of them can be addressed but not all of them
	• It is unclear who owns the data
	• One provider's SaaS application can be based on another provider's PaaS solution that runs on other provider's IaaS offering, which adds another level of security risks and becomes difficult to trace whether or not legislation and internal security policies are met
	• Many cloud providers claim that they are compliant with security standards, but enterprises want to make sure that this is of relevance to the kind of security they are looking for
	• Insufficient and inconsistent data encryption policies and practices
	• Real security risks related to data theft, hacking, virus attacks, data corruption. Especially, if the hypervisor layer got compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding that

	• Lack of trust in the cloud's multi-tenancy architecture and the governments of countries where the data is stored. Thus, data need to be encrypted to make it hard to use customer data in case of data leakage
	• Enterprises in a certain geographical location trust in, or forced by the government to deal with, cloud providers within their area whether they provide the best service or not. While these providers might be using 3rd party providers to store the data
	• The security department involvement is important at every step of the migration, from the requirements gathering, the technical implementation and till the support cycle is in production and running
	• The concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impact on productivity
	• Each team/department/organization adopting their own concept of a cloud and it becomes difficult to migrate all the clouds into one big cloud
	• Lack of uniform support models makes it complex to integrate cloud solutions with the legacy on-premise IT infrastructure as well as data from different sources which costs effort and time and may affect applications availability and data integrity
	• Lock-in concern about taking back the data and software from one cloud vendor to another, if the service is not satisfactory, without affecting business operations
	• If the cost of using cloud services is not lower than on-premise, it is difficult to get the cloud strategy supported by the management
	• Little investment costs when transferring to a cloud solution but must expect a higher monthly rate
	• Data protection legislations are different and not strong in all countries
	• Compliance with data privacy Acts is mandatory and it may slow investing in and exploiting the full benefits of cloud services
	• Laws and standards are difficult for companies to get an overview of them and make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects
	• Enterprises are faced with weak undetailed Service Level Agreements (SLAs) from providers (e.g., providers may not be transparent about where and how do they store the data and the acknowledgement of security incidents whenever happen and how the cloud provider deals with it)
	• It is hard for small clients to modify the standard agreements of major international cloud providers
	• People being used to old systems will have to change how they work (more automation, less paperwork, new routines etc), and this is hard for many people and should not be underestimated

	• The meaning of cloud, the difference between it and on-premise, and the consequence of using it is not clear for the users (including managers) which may weaken its value
	• Implementing cloud services in your organization requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers) which can be expensive and time-consuming, especially, in implementing private clouds
	• User support is a critical component in building trust between business operations and IT services
	• Failure to modify business processes in order to leverage the effect of cloud computing agility on the business model
	• The concern that the transition to the cloud doesn't disturb current IT and Business operations
	• The company is dependent on external routines and competence and if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal duties
	• Lack of IT governance tools, policies, and best practices particular to cloud service management
	• It is important to adopt cloud service models that have a degree of maturity, so that sensitive data and functions can be implemented in private cloud, otherwise, MUST be kept on-premise. While non-sensitive data and functions can be outsourced to the cloud
	• Lack of reaching an agreement about cloud adoption strategy at all levels can kill of the best-intended initiative
	• Plans for dealing with incidents (downtime, provider goes bankrupt, and the data center is destroyed) should be in place to keep business critical operations running

2. Comments or Justifications on Rankings

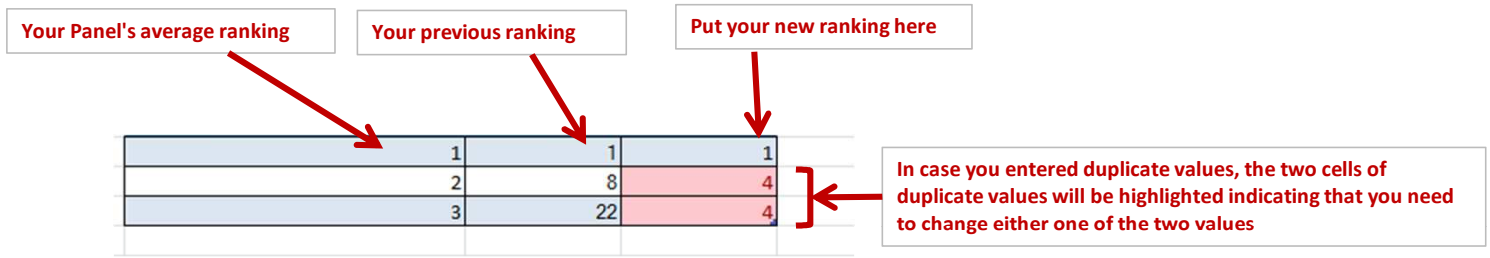
Delphi study on Cloud Computing - Re-Ranking Questionnaire

From the previous round of ranking we did not reach the required level of agreement. One of the purposes in a ranking-type Delphi study is to obtain consensus among the participants. We have a quite low value regarding consensus (low Kendall W value). Therefore we need to do a new ranking round. This is very important for completing the study and for increasing the validity of the results.

Based on the average ranking of the issues on the list, we have now reduced the list from 33 issues down to the top 18 issues. We ask you to kindly review this list and do ranking adjustments if you do not agree. Your previous ranking list is also presented for you to compare with the average. See the table provided in excel sheet named "Re-ranking issues". If you wish to justify your new ranking, or give feedback/comments, please use the "Comments/Justification" area placed beside the table.

PS. To clarify: To keep your first ranking of some of the issues as it is – is an option as long as it is within the range from 1 to 18 for consistency, to agree on the average ranking of your panel– is also an option. All alternatives between these two are also possible. Since average top 18 issues are considered, you may not find all your top 18 from the first round. The purpose of this round is to increase the degree of consensus within each sub-panel.

We share comments from some of the experts from the previous ranking round in the excel sheet named “Comments from previous round”.



Issues are listed by category and placed between parentheses	Provider Panel Average Rankings	Your Ranking	New Ranking
Security (The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than public clouds. However, risks are not absolute and most of them can be addressed but not all of them)	1	16	
Strategy (Plans for dealing with incidents (downtime, provider goes bankrupt, and the data center is destroyed) should be in place to keep business critical operations running)	2	4	
Security (Lack of trust in the cloud's multi-tenancy architecture and the governments of countries where the data is stored. Thus, data need to be encrypted to make it hard to use customer data in case of data leakage)	3	29	
Strategy (Lack of reaching an agreement about cloud adoption strategy at all levels can kill of the best-intended initiative)	4	2	
Strategy (It is important to adopt cloud service models that have a degree of maturity, so that sensitive data and functions can be implemented in private cloud, otherwise, MUST be kept on-premise. While non-sensitive data and functions can be outsourced to the cloud)	5	10	
Legal and ethical (Laws and standards are difficult for companies to get an overview of them and make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud computing aspects)	6	20	
IT Governance (Lack of IT governance tools, policies, and best practices particular to cloud service management)	7	18	
Migration (Lock-in concern about taking back the data and software from one cloud vendor to another, if the service is not satisfactory, without affecting business operations)	8	17	
Culture (People being used to old systems will have to change how they work (more automation, less paperwork, new routines etc), and this is hard for many people and should not be underestimated)	9	12	
Legal and ethical (Data protection legislations are different and not strong in all countries)	10	14	
Migration (Lack of uniform support models makes it complex to integrate cloud solutions with the legacy on-premise IT infrastructure as well as data from different sources which costs effort and time and may affect applications availability and data integrity)	11	32	
Legal and ethical (Compliance with data privacy Acts is mandatory and it may slow investing in and exploiting the full benefits of cloud services)	12	31	
Legal and ethical (Enterprises are faced with weak undetailed Service Level Agreements (SLAs) from providers (e.g., providers may not be transparent about where and how do they store the data and the acknowledgement of security incidents whenever happen and how the cloud provider deals with it))	13	25	
Security (The security department involvement is important at every step of the migration, from the requirements gathering, the technical implementation and till the support cycle is in production and running)	14	19	
Business (Little investment costs when transferring to a cloud solution but must expect a higher monthly rate)	15	1	
Security (Using public cloud services (Bring Your Own Cloud - BYOC) for project collaboration may threaten employees' personal data and business confidential data and makes it difficult to maintain and control a security policy for access and distribution of corporate information)	16	28	
Security (Many cloud providers claim that they are compliant with security standards, but enterprises want to make sure that this is of relevance to the kind of security they are looking for)	17	22	
Awareness (The meaning of cloud, the difference between it and on-premise, and the consequence of using it is not clear for the users (including managers) which may weaken its value)	18	9	

Comments/justifications

Comments/justifications

Comments From Previous Ranking	Said by
In short, It seemed logical to me to place security as the top concern, legalization second followed by network performance. My concerns were on the legacy policies and processes as well as the fear of poor adoption to the cloud in terms of restructuring or end-user experience.	Client
The criticality of business transition, laws and regulations, security etc are impacted by which cloud software you are talking about. Some solutions are much more critical and sensitive to the business than others. Difficult to rank without having any borderlines or differentiation between SW products.	Provider
Biggest concern is the lack of governance that manages both on-premise and off-premise resources. Lack of an appropriate legal and regulatory framework for international information commerce via cloud computing platforms contribute to this issue. This environment makes it difficult for organizations to establish a strategy and drives a lack of conscientious or shared knowledge about cloud.	Provider
Here are some feedback and concerns regarding the investigation: It is a big difference regarding concerns – it depends upon if you discuss private, public or hybrid cloud solutions. This investigation does not separate on this, and each participants will answer dependent upon which cloud solution they have. We have our concerns/worries in relation to the private cloud solution which we are building now, however, our concerns are something else when we consider the opportunities for hybrid cloud solutions. To implement public cloud solutions on a large scale, is per now not a solution we consider because of - among other – law and rules. Some of the concerns are overlapping, however some of them we think will be addressed if we choose to establish a hybrid cloud solution. That means we will not implement a hybrid solution if it is not committed in the organization – with respect to which services there should be in the cloud. Another thing – we need to have trust to the vendors – if they satisfy our requirements regarding security, processes and routines that ensure a stable operation and up-time according to SLAs. In big lines our concerns are: 1) security (integrity, confidentiality, availability), 2) Governance, organizing, processes and routines. Changes in work task will follow and also new competence requirements for the organization will turn up. That will influence both managers and employees. You will need competence regarding ordering and how to follow-up the external vendors who need to customize the cloud solutions. It follows that there are new requirements that must be in place in the SLAs, and which need to be handled and followed up. We must have competence on this – to be able to state our demands, and know which demands/requirements we need to state, and how to follow up these requirements.	Client

Sample Key Interview Questions

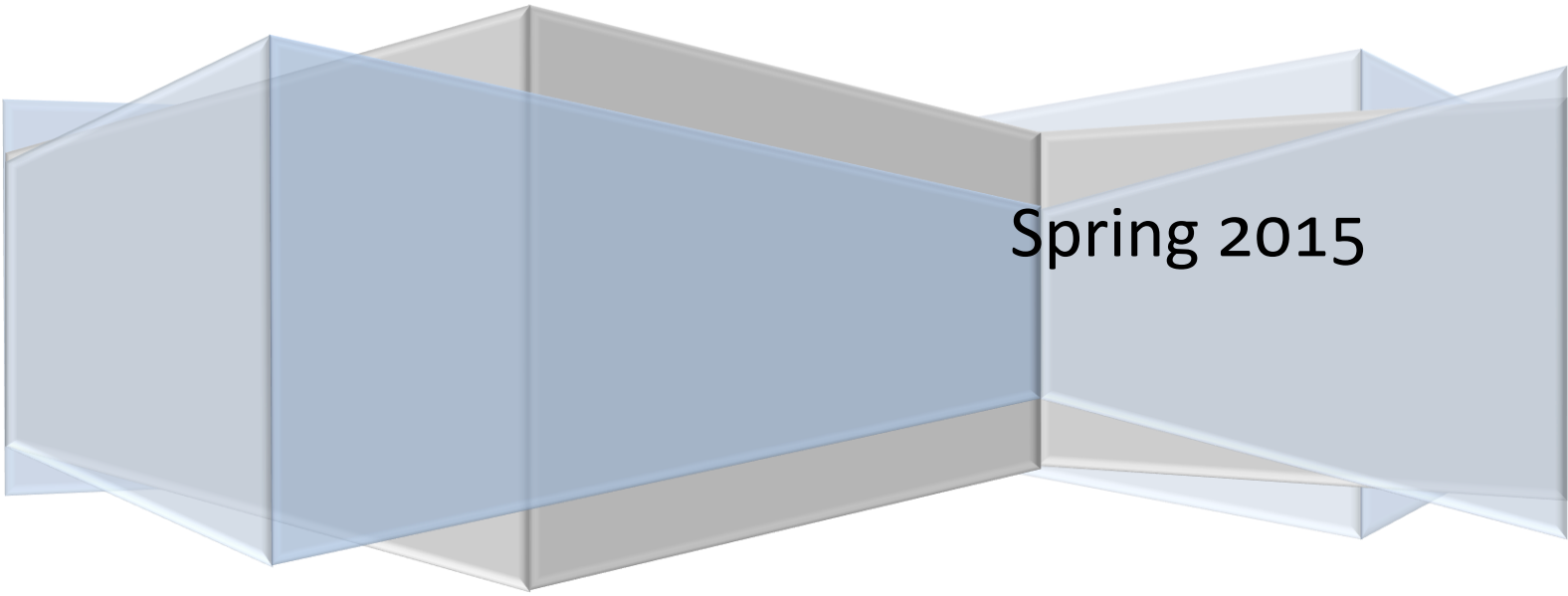
1. Why do you think enterprises started to use cloud services?
2. Is the legal framework sufficient to enable the use of cloud services? Or there still more regulations need to be in place?
3. What are the issues with security and regulations?
4. What are the sources of underestimation of change?
5. How do you see the problem of responsibility for sensitive data?
6. What do you recommend for companies deciding to move to the cloud? What aspects they have to look into?
   Is the communication infrastructure ready enough in Egypt for cloud computing in terms of connectivity?
   What makes enterprises afraid of cloud computing?
7. Do you think there are ready policies in the organization to meet whatever security challenges regarding the cloud?
8. What are the problems in integrating the cloud environment with already existing systems?
9. Do you think there is major change in required skills to be cloud ready?
10. Are you using the cloud already? Or deciding?
11. Why did you go to the cloud?
12. Have you faced clarity issues with cloud providers?
13. What do you need to know as a client to close the knowledge about the cloud and the consequences of its use?

UNIVERSITY OF AGDER
FACULTY SOCIAL SCIENCES

Adoption of Cloud Computing

Results from a Delphi Study

The report is part of a research project at University of Agder
Department of Information Systems
prepared by
Rania Fahim H.I. Elgazzar (Doctoral Candidate)
Eli Hustad (Associate Professor)
Dag H. Olsen (Professor)



Spring 2015

Contact: rania.f.el-gazzar@uia.no

Preface

This report derives from a research project carried out at the University of Agder, Department of Information Systems. The study is part of Rania Fahim H.I. Elgazzar's doctoral project, which focuses on the adoption of cloud computing in enterprises. The results of this report stem from a Delphi study, in which 34 experts from different industries and public institutions participated. We gratefully acknowledge all the panelists who made this study possible and contributed with their knowledge and engagement in several rounds of sampling. We also express our gratitude to the experts who also participated in follow-up interviews.

Kristiansand, Norway, May 8 2015

Rania Fahim H.I. Elgazzar

Eli Hustad

Dag H. Olsen

Executive Summary

Topic: The adoption of cloud computing services is influenced by many issues perceived differently by clients and cloud service providers; providers may see the positive side of the cloud, whereas clients may perceive it otherwise. This report presents the results of a Delphi study and focuses on the following two questions: *What issues confront enterprises when adopting cloud computing services? What is the relative importance of these issues?*

Method: Thirty-four experts from different industries and public institutions participated in a Delphi panel. It was divided into three subpanels that represent different stakeholders, namely, clients, providers, and academics. We started the study in 2013 and completed it in March 2015. The Delphi study procedure comprised three stages, namely, (1) brainstorming, (2) narrowing down, and (3) ranking. Follow-up interviews were also conducted to gain an in-depth understanding of the topics examined.

Findings: The panelists identified 55 issues of concern in the first round, and these were analyzed and grouped into 10 categories: (1) security, (2) availability, (3) migration, (4) business, (5) legal and ethical concerns, (6) culture, (7) awareness, (8) impact, (9) strategy, and (10) IT governance. In the second round, most of the panelists' votes went to security (104 votes), followed by legal and ethical (67 votes), impact (60 votes), and strategy (54 votes) issues. In the narrowing down phase, 33 issues were identified, and these were based on a threshold of 30%. In the first ranking round, 33 issues were ranked by the panelists. However, we could not reach an acceptable agreement (Kendall W was for clients=0.173, providers=0.069, and academics=0.270). In the second round of ranking, the top 18 issues of each subpanel were ranked, and the intrapanel agreement showed moderate consensus on the issues (Kendall W was for clients=0.392, providers=0.443, and academics=0.493). We found that the client panel ranked the issue "Data protection legislations are different and not strong in all countries" as number one, the provider panel ranked the issue "The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that in public clouds. However, risks are not absolute, and most of them can be addressed, but not all of them" as number one, and the academic panel ranked the issue "Enterprises are faced with weak undetailed Service Level Agreements (SLAs) from providers (e.g., providers may not be transparent about where and how do they store the data and the acknowledgement of security incidents whenever happen and how the cloud provider deals with it)" as number one. Follow-up interviews were also conducted. The insights of the panelists are shared in this report.

Conclusions: The report highlights current cloud computing adoption issues. Security, strategy, legal and ethical concerns, and IT governance were among the highest-ranked issues by the participants in the study. The results show different perspectives across the subpanels, especially for the clients and providers. Clients need to understand well their business needs and what value cloud computing can add to their business. Cloud service providers need to fully comprehend the current needs of their market. More work needs to be done on increasing awareness regarding cloud computing and its benefits for businesses. Clients are particularly interested in hearing more about hybrid cloud solutions. The most important issues of concern are further discussed in this report.

Content

Executive Summary 2
1. Introduction to the Study 4
2. Key Concepts of Cloud Computing 5
3. About the Study 6
3.1 Sample Description 7
4. Study Procedures 9
4.1 The Brainstorming Phase 9
4.2 The Narrowing-down Phase 13
4.3 The Ranking Phase 13
4.4 The Interviews 14
5. Main Results of the Study 14
6. Discussion of Results 19
References 21
7. Appendix 1 23
7.1 Detailed results from the brainstorming phase 23
7.1.1 Security issues 24
7.1.2 Availability issues 25
7.1.3 IT governance issues 25
7.1.4 Migration issues 26
7.1.5 Business issues 27
7.1.6 Legal and ethical issues 28
7.1.7 Cultural issues 29
7.1.8 Awareness issues 29
7.1.9 Impact issues 30
7.1.10 Strategy issues 31

1. Introduction to the Study

While the cloud-computing market is growing, scholars and practitioners alike are debating about the pros and cons of this technology. Especially among small- and medium-sized enterprises (SMEs), the interest in utilizing these services has drawn increasing attention, and around 60% of SMEs have already purchased at least one cloud service (Avrane-Chopard, Borgault, & Moodley, 2014).

Despite the fact that several benefits of cloud computing are well known and documented, enterprises are still concerned about the risks and consequences when moving business-critical applications to the cloud. For instance, these issues comprise the distributed nature of cloud computing, including security and privacy threats, national and international regulations, and the external business environment where the enterprise operates (Armbrust et al., 2009). A main critique of cloud computing is that the security cost, privacy, and availability concerns may outweigh its benefits (Kshetri, 2013). Several surveys have concluded that the security concern in particular is the most serious barrier to cloud-computing adoption within enterprises (Kshetri, 2013, Table 1, p. 2).

However, there seems to be a gap between how user organizations and cloud service providers (CSPs) view the benefits of and concerns about cloud services. While the vendors underscore that data are most secure when stored in external data centers, the users are worried about the ambiguities around security and confidentiality when business-critical or highly sensitive data are stored outside their own walls (Goodburn & Hill, 2010).

Thus, there is a need to gain more insights about these uncertainties. This study aimed to identify *which issues were of most concern* when enterprises considered adopting cloud-computing services.

We asked 34 experts from different industries and public institutions for their opinions on the following questions:

What issues confront enterprises when adopting cloud-computing services?

What is the relative importance of these issues?

The 34 experts were invited to participate in a ranking-type Delphi study. The Delphi method is a sampling approach that is appropriate for "identifying and prioritizing issues for managerial decision-making" (Okoli & Pawlowski, 2004, p.1).

The 34 experts constituted a so-called Delphi panel. The panelists (participants) were divided into three subpanels: (1) clients (representing cloud-computing user organizations), (2) providers (representing CSPs, vendors, partners, brokers, consultants, or similar parties), and (3) academics (representing academics from different educational institutions focusing on cloud computing in their own research). The purpose of having

three groups was to reveal the potential for different perceptions of cloud-computing adoption among various stakeholders.

The report is organized as follows. First, we present some key concepts of cloud computing. Second, we explain how we conducted the Delphi study. Third, we present our main results; finally, we discuss them.

2. Key Concepts of Cloud Computing

Cloud computing represents a new paradigm in computer system solutions and has received increasing interest in recent years (see e.g. Armbrust et al., 2010; Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009; Saya, Pee, & Kankanhalli, 2010; Sultan, 2011). Cloud computing refers to the various services delivered over the Internet (X-as-a-service), where X can be the platform, infrastructure, or software (Armbrust et al., 2009). Data processing and storage are remotely controlled and take place on remote servers. Users do not need to store applications or data locally on their machines. Internet services (Web services) and service-oriented architecture are important building blocks for cloud computing (Vouk, 2004), in addition to functionality based on virtualization and grid computing (Sultan, 2011).

The development of cloud services has increased in recent years, and business systems delivered as cloud solutions have become part of the market (Vmware, 2011). According to the Gartner Group, cloud-computing solutions are still immature technologies (Pettey & Stevens, 2009), which have not achieved stabilization or a critical mass of users.

Buyya et al. (2009) conceptualize cloud computing as follows: "*A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers*" (p. 3). They conjecture that cloud computing represents the next generation of data centers, consisting of connected and virtualized machines (VMs). Access to services and resources will be based on agreements between service providers and customers. Cloud computing will be considered the fifth "utility" (infrastructure service), after water, electricity, telephone, and gas. Users hook up to the cloud via the Internet and rent computing resources in the same way as they are connected to electricity and the telephone and pay for services based on usage.

Through Internet-based applications, users have access to resources via a web browser in the same manner as if the applications were installed locally on a PC. Such solutions have advantages because they are easy to scale up to many users. The system architecture associated with cloud computing involves several components that communicate with one another via various application programming interfaces (APIs). These APIs are often Internet services such as the Simple Object Access Protocol (SOAP, a platform-independent protocol) and a three-layer architecture. Front-end solutions in cloud

computing represent the network and applications that are visible to the user via a web browser, while the back end represents the cloud, consisting of various computers, servers, and storage devices, invisible to the user (Armbrust et al., 2010).

Examples of cloud solutions are platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), and software-as-a-service (SaaS). The PaaS represents the technology that generates all the properties required to support the development process and delivery of web-based software (Jensen, Schwenk, Gruschka, & Iacono, 2009). The National Institute of Standards and Technology (NIST) defines PaaS as a solution that gives users the opportunity to upload self-developed code or download applications located in a cloud infrastructure (Mell & Grance, 2011). However, the user does not control the underlying infrastructure, such as servers, networks, and operating systems. One example of PaaS is the Azure platform (Microsoft, 2011).

The IaaS provides computer resources, such as servers, connections, storage, and other tools necessary to build an application design for various organizations (Sultan, 2011). It is a solution that supports data processing and storage; users can post their own applications or download others. Users have no control over the underlying infrastructure, but they control the software and operating system. An example of IaaS is Amazon (Amazon, 2011).

Finally, SaaS is a delivery method for applications. Suppliers have applications stored on their servers, which are made available to customers through a web browser. Users have no control over the underlying technology, such as servers, operating systems, databases for storage, or properties in the application. Examples of SaaS solutions are enterprise resource planning (ERP) solutions in the cloud (e.g. Xledger.net, 2015) and customer relationship management (CRM) systems that are delivered via cloud services (e.g. Salesforce, 2015).

There are several delivery models for cloud computing (Mell & Grance, 2011). In a public cloud, the technology is available to all or adapted to an industry. The supplier owns the system solution for the service. A public cloud consists of a group of companies with similar interests that collaborate to manage a cloud or platform. A private cloud can also be created for a particular company and can be operated by the organization itself or outsourced to other suppliers. In a hybrid cloud, public and private cloud services are combined.

3. About the Study

The purpose of the study was to explore the different concerns perceived by various stakeholders regarding cloud-computing adoption.

3.1 Sample Description

The experts were grouped into three subpanels: clients, providers, and academics. They were selected from different countries (6), industries (13), company types (public or private), company sizes (large, SME, and micro), and roles (5). The distribution of the experts across these criteria is visualized in the following graphs (Figures 1–5).

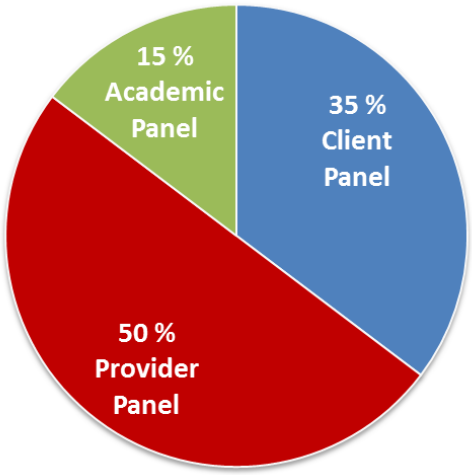


Figure 1. Distribution of participants according to the different subpanels

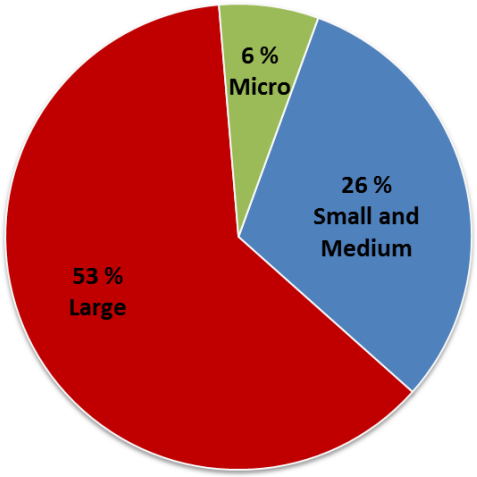


Figure 2. Distribution of participants according to company size

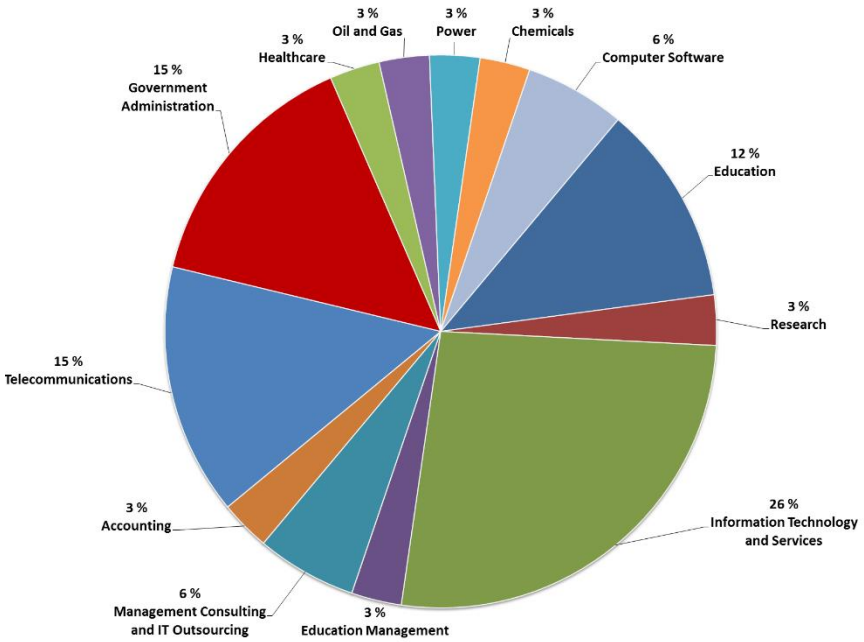


Figure 3. Distribution of participants according to industries and institutions

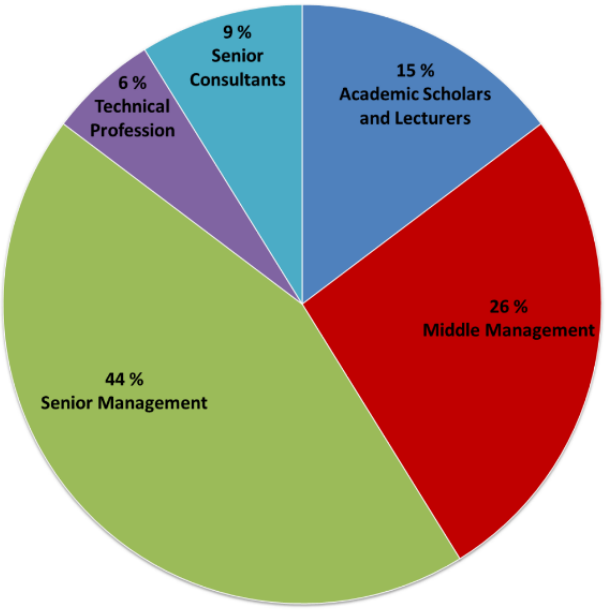


Figure 4. Distribution of participants according to their respective roles in their organizations

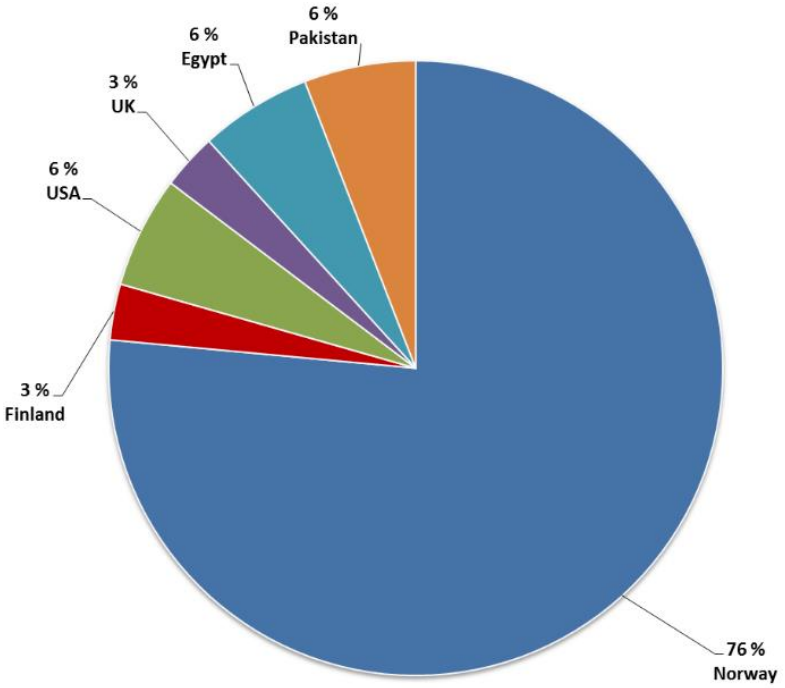


Figure 5. Distribution of participants according to location

4. Study Procedures

This study primarily aimed to reveal the most important issues that enterprises would need to consider in their decision-making processes regarding adoption of cloud-computing services. The second purpose was to prioritize the issues of most concern by conducting a "ranking-type" Delphi study (Schmidt, 1997). The ranking part of the study was important for consensus building within the panel (Hsu & Sandford, 2007); this was attained by reaching agreement on the order of these issues' importance among distinct stakeholders.

Thirty-four experts agreed to participate in the study.

The study comprised the stages of brainstorming, narrowing down, and two rounds of ranking. Additionally, we conducted interviews with 16 participants in the panel.

Figure 6 shows the process of the Delphi study. In the following sections, we explain how we performed the different stages of the study.

4.1 The Brainstorming Phase

In the brainstorming phase, an open-ended question was sent to each of the experts by email: *"What are the issues that enterprises are confronted with when adopting cloud-computing services?"* We asked them to provide at least six issues to answer our question. They were asked to specify each issue, justify its importance and consequences, and if possible, add comments to elaborate on it. Based on the experts' statements and explanations, the authors of this paper analyzed the material generated by the panelists. The analysis sought to identify the most important issues; through this work, we combined similar issues and removed duplicate meanings. In total, 55 different issues were identified, which were further systemized and grouped into 10 main categories.

Table 1 shows the main results from this phase of the study.

In addition, Appendix 1 presents more details from this phase and how issues were voted differently among the subpanels. The weighting of the issues made the foundation for doing the narrowing-down analysis (30% threshold).

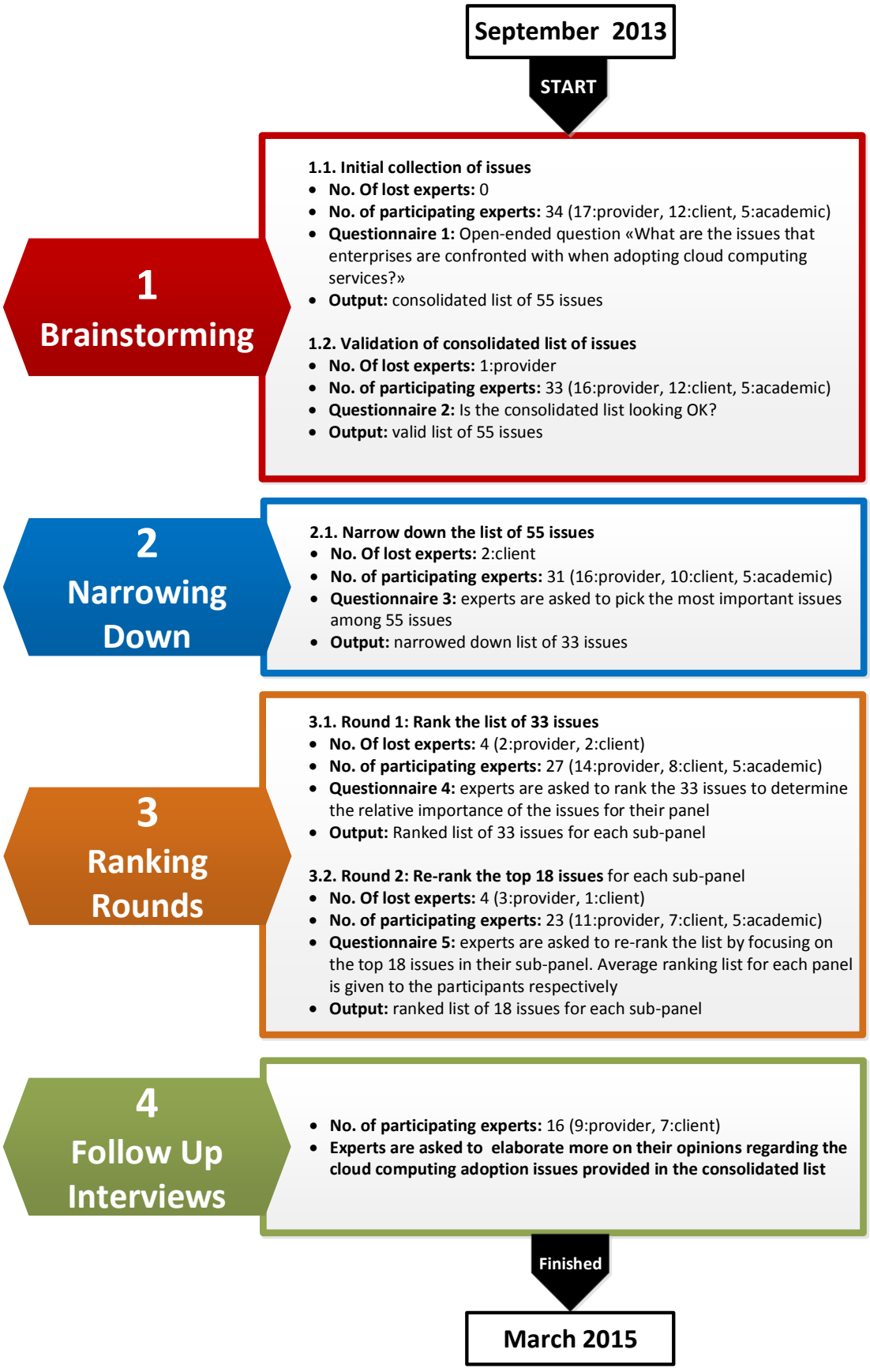


Figure 6. The process of the Delphi study

Table 1. List of 55 issues identified by the experts and grouped into 10 main categories

Category	Issues
1. Security (14 issues)	• Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.
	• The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.
	• The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.
	• It is unclear who owns the data
	• Malicious insiders (i.e., cloud provider's employees) may access the cloud servers and steal confidential data of the cloud users.
	• One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.
	• Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.
	• There may be insufficient and inconsistent data encryption policies and practices.
	• There are real security risks related to data theft, hacking, virus attacks, and data corruption. Specifically, if the hypervisor layer becomes compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding these issues.
	• There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.
	• There is concern about making the data lifecycle secure in all its phases (i.e., create, store, use, share, archive, and destroy). An insecure data lifecycle may lead to data leakage. Regarding data deletion, if the provider does not provide proof that its data-wiping technique prevents data recovery, this will put customer data (i.e., financial data, employee records, or medical records) at risk, causing confidentiality problems, thus affecting the enterprise's reputation.
	• Multiple tenants may disrupt services unintentionally, causing a denial of service (DoS) attack that makes services unavailable, which leads to losing customers.
	• Enterprises in a certain geographic location trust in or are forced by the government to deal with cloud providers within their area, whether they provide the best service or not. On the other hand, these providers might be using third-party providers to store the data.
	• The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.
2. Availability (1 issue)	• There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity.
3. Migration (3 issues)	• Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.
	• The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.
	• There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.
4. Business (9 issues)	• If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.
	• Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.
	• The transition from capital expenditure to operational expenditure reduces operational margins but increases operational risks and could lead to a less predictable cost level.
	• Cloud solutions are difficult to sell because they are not supported by traditional sales models.
	• Cloud computing offers financial benefits and very well-articulated services but results in a higher total cost of ownership (TCO).
	• Budget constraints may lead to delays in implementing current visions. It has to be clear to the top management how much money can be saved in the future when spending so much at once.
	• There is fear of losing business and long-term brand recognition.
	• The slow development of suitable standards causes the lack of technological innovation within the cloud industry.
	• A significant amount of negative marketing exists in cloud services.
	• Data protection legislation is different and not strong in all countries.

Category	Issues
5. Legal and ethical (7 issues)	• Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.
	• It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud-computing aspects.
	• Standardized cloud-process models do not support customization, and organizations may have to change their processes and practices to maximize the benefits.
	• Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).
	• There is no standard service level agreement (SLA) for cloud-computing delivery methods due to unsolved security and environmental (such as supplier dependency) issues, which will lead to unclear segregation of duties between the cloud provider and the consumer (due to the lack of legal precedents) regarding responsibilities for personal and sensitive business data at the level of the service models, IaaS, PaaS, and SaaS). This raises potential security vulnerabilities.
	• It is hard for small clients to modify the standard agreements of major international cloud providers.
6. Culture (2 issues)	• People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.
	• Some key people in the organization are powerful, and management may fear confronting them with change if they strongly oppose it.
7. Awareness (4 issues)	• The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.
	• There is reluctance to adopt a cloud service with less functionality or reduced user experience (efficiency and flexibility) than that of traditional solutions.
	• The consumer's lack of security awareness results in misuse of the cloud environment and misconfiguration of the cloud-environment layers.
	• There is a lack of analysis and sales activities as some vendors deliver IaaS as though it should be a pure public cloud. However, when clients more closely examine how vendors deliver their services, these do not fulfill customer expectations (some services are not automatically created, which cost effort and money to create) and turn out to be more like traditional outsourcing that is packed as a cloud service, sales wise.
8. Impact (7 issues)	• Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.
	• User support is a critical component in building trust between business operations and IT services.
	• Organizations may fail to modify their business processes to leverage the effect of cloud-computing agility on business models.
	• There is concern about whether the transition to the cloud disturbs current IT and business operations.
	• Cloud computing offers an opportunity for reorganizing the IT department (laying off dedicated staff).
	• Maintaining an old organizational chart will lead to gaps in understanding new requirements from all involved teams.
	• The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.
9. IT Governance (1 issue)	• There is a lack of IT governance tools, policies, and best practices particular to cloud-service management.
10. Strategy (7 issues)	• It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it *must* be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.
	• The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.
	• There is a huge variance in the demands for each organization/department/employee. Thus, the chosen model(s) have to serve all needs in the most efficient way compared to the traditional methods.
	• In many cases, the adoption is more "random," and the benefits disappear because key considerations are overlooked (in terms of what organizations actually want, what they expect, why they want to adopt the cloud, what can be implemented in the cloud, and how to transition).
	• Each organization is required to describe its enterprise architecture in detail to easily contract the correct cloud services for the "to-be" architecture.
	• Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.
	• It is important to evaluate the provider (in terms of experience with the industry, ability to provide advice on "cloud orchestration," operational stability, and long-term commitment) and ensure that prices are comparable across different vendors.

4.2 The Narrowing-down Phase

The purpose of this phase was to reduce the list of issues to focus on the most important ones and to make the list manageable for ranking the items. The experts were asked to select 10 (minimum) to 20 (maximum) issues that they believed were most important to them. At this stage, we decided to analyze the subpanels separately. We noticed differences among the subpanels in prioritizing the issues; thus, we wanted to highlight these differences in addition to analyzing the combined panel's results. We analyzed the results by using 30% as the threshold to consider the most important issues for the experts in each subpanel. This resulted in a list of 33 issues ready for ranking. By comparing the results of the brainstorming stage (identification of issues) with those of the narrowing-down (selection of most important issues) phase, the reduction analysis provided: (1) security (identified = 14 issues, selected = 11 issues), (2) availability (identified = one issue, selected = one issue), (3) migration (identified = three issues, selected = three issues), (4) business (identified = nine issues, selected = two issues), (5) legal and ethical concerns (identified = seven issues, selected = five issues), 6) culture (identified = two issues, selected = one issue), (7) awareness (identified = four issues, selected = one issue), (8) impact (identified = seven issues, selected = five issues), (9) IT governance (identified = one issue, selected = one issue), and (10) strategy (identified = seven issues, selected = three issues).

4.3 The Ranking Phase

In this phase, a randomly arranged list of 33 issues was sent to each of the experts for ranking. The purpose was to decide the relative importance of the issues. To measure the degree of consensus among the experts in each subpanel, we calculated the mean ranking and Kendall's coefficient of concordance (W) for each subpanel. The value of Kendall's W provides a measure of the consensus among the panel participants. We could not reach the level of concordance of $W = 0.7$ that is considered an indication of a high level of agreement for Delphi studies (Schmidt, 1997). ($W = 1.0$ means full agreement in the panel regarding the order of the ranked issues). The Kendall W values showed low levels of agreement for all three subpanels: academics (0.270), clients (0.173), and providers (0.069).

We decided to conduct a new ranking round, aiming to increase Kendall's W to be more precise regarding *the relative importance* among the issues identified. The first round gave us an indication of which of the 33 issues were most important, and it was now easier to reduce the number of issues. We decided to focus on the top 18 issues, based on the mean ranking for each subpanel. The feedback from the first round of ranking gave us an impression of the difficulties in ranking too many issues, so by reducing the number of issues, it would be easier for the participants to focus on the most important issues for them. Since each subpanel had ranked the 33 issues quite differently, it was important to keep the subpanels separate and focus on the top 18 issues for each of them.

4.4 The Interviews

The purpose of the interviews was to enrich and contextualize the existing data achieved from the Delphi study. The interviews supported the findings from the Delphi ranking and provided more insights and deeper explanations of the issues identified through elaborations from the interviewees.

5. Main Results of the Study

Table 2 depicts the results of the second round of ranking, which determined the relative importance of the top 18 issues for each subpanel. The relative importance of issues was ranked differently among the subpanels. By comparing the rankings across the subpanels, we observed a low consensus for the panel as a whole (low interpanel agreement). Kendall's *W* was 0.199. Each subpanel showed a moderate degree of consensus according to Kendall's *W*, which was in the 0.4–0.5 range. This indicated a moderate intrapanel agreement for all three subpanels.

Examining the combined ranking (CR) shows the dominant issues related to four specific categories; security, strategy, legal and ethical concerns, and IT governance were leading (e.g., among the top nine issues). For each subpanel, the clients (C) mostly agreed on the CR regarding the main categories of importance, while the providers (P) also emphasized the categories of culture (CR = 11; C = not ranked (÷), **P = 6**, A = ÷), and migration (CR = 14; C = ÷, **P = 9**, A = ÷). The academics (A) additionally highlighted the category of impact (CR = 16; C = 16, P = ÷, **A = 6**).

Table 3 shows the results organized by category and the related issues.

In the next section, we discuss the most important results based on the rankings and the data from the interviews.

Table 2. Ranking results - combined ranking and ranking for each subpanel, organized by priority of combined ranking

CR*	Issues	C (N = 7)	P (N = 11)	A (N = 5)	Category
1	The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.	3	1	2	Security
2	Data protection legislation is different and not strong in all countries.	1	10	3	Legal and ethical
3	Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.	7	2	12	Strategy
4	There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.	6	3	15	Security
5	It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it *must* be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.	8	4	10	Strategy
6	Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.	5	11	4	Legal and ethical
7	Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).	13	13	1	Legal and ethical
8	Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.	2	17	11	Security
9	There is a lack of IT governance tools, policies, and best practices particular to cloud-service management.	17	8	17	IT governance
10	It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud-computing aspects.	15	5	÷	Legal and ethical
11	People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.	÷	6	÷	Culture
12	The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.	÷	7	÷	Strategy
13	The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.	14	15	÷	Migration
14	There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.	÷	9	÷	Migration

15	The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.	9	÷**	8	Impact
16	There is concern about whether the transition to the cloud disturbs current IT and business operations.	16	÷	6	Impact
17	The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.	÷	14	16	Security
18	The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.	÷	18	9	Awareness
19	The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.	4	÷	÷	Security
20	Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.	11	÷	14	Impact
21	Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.	÷	12	÷	Business
22	It is unclear who owns the data.	÷	÷	5	Security
23	Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.	÷	16	÷	Security
24	There may be insufficient and inconsistent data encryption policies and practices.	10	÷	÷	Security
25	It is hard for small clients to modify the standard agreements of major international cloud providers.	÷	÷	7	Legal and ethical
26	If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.	12	÷	÷	Business
27	One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.	18	÷	÷	Security
28	Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.	÷	÷	13	Migration
29	There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity.	÷	÷	18	Availability
0.199	**Kendall's *W***	**0.392**	**0.443**	**0.493**	

*CR = combined ranking (total of 29 issues for all three subpanels).

**The symbol ÷ indicates that the issue was not among the top 18 issues for this particular subpanel.

Table 3. Ranking results – combined ranking and ranking for each sub-panel, organized by category

CR*	Issues	C (N=7)	P (N=11)	A (N=5)	Category
1	The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.	3	1	2	Security
4	There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.	6	3	15	Security
8	Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.	2	17	11	Security
17	The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.	÷	14	16	Security
19	The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.	4	÷	÷	Security
22	It is unclear who owns the data.	÷	÷	5	Security
23	Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.	÷	16	÷	Security
24	There may be insufficient and inconsistent data encryption policies and practices.	10	÷	÷	Security
27	One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.	18	÷	÷	Security
2	Data protection legislation is different and not strong in all countries.	1	10	3	Legal and ethical
6	Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.	5	11	4	Legal and ethical
7	Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).	13	13	1	Legal & Ethical
10	It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud-computing aspects.	15	5	÷	Legal and ethical
25	It is hard for small clients to modify the standard agreements of major international cloud providers.	÷	÷	7	Legal and ethical

3	Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.	7	2	12	Strategy
5	It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it *must* be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.	8	4	10	Strategy
12	The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.	÷	7	÷	Strategy
15	The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.	9	÷	8	Impact
16	There is concern about whether the transition to the cloud disturbs current IT and business operations.	16	÷	6	Impact
20	Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.	11	÷	14	Impact
9	There is a lack of IT governance tools, policies, and best practices particular to cloud-service management.	17	8	17	IT governance
11	People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.	÷	6	÷	Culture
13	The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.	14	15	÷	Migration
14	There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.	÷	9	÷	Migration
28	Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.	÷	÷	13	Migration
21	Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.	÷	12	÷	Business
26	If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.	12	÷	÷	Business
18	The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.	÷	18	9	Awareness
29	There is concern about assuring appropriate connectivity for enterprises and their customers to avoid negative impacts on productivity.	÷	÷	18	Availability
0.199	**Kendall's *W***	**0.392**	**0.443**	**0.493**	

6. Discussion of Results

This study aimed to examine the most important issues related to cloud-computing adoption. The interviews support the findings from the Delphi ranking and provide us with a deeper understanding of the issues. We briefly discuss the most significant findings below.

First, issues related to security and risks dominate the rankings, which are corroborated by the interviews. The risks stem from the fundamental aspects of cloud computing, such as data transfer over the Internet, remote data hosting, and virtualized and shared resources.

The most important issue ("the risk of losing control over resources …") reflects an overarching perspective on the gamut of risks that are or can be associated with cloud computing. Many of the other top-ranked issues are related to this one. The second highest-ranked item among the providers ("plans for dealing with incidents …"; C = 7, P = 2, A = 11) is about strategies for dealing with incidents, which may occur due to risks implicit in the cloud-computing model. Likewise, several of the highest-ranked items can also be perceived as manifestations of the same overarching security and risk issues, from a security, strategic, or legal and ethical perspective.

Our study reveals that most clients invest in cloud services as local initiatives, without concern about the integration with the enterprise systems and IT infrastructure. This tendency to bypass IT departments is one of the most significant security risks (Cloud Security Alliance, 2013) and undermines security policies at the business level. We have also observed the clients' general lack of sufficient proficiency in their data security governance; often, they do not even know which questions to ask. We conjecture that expert security governance must be in place before most client companies will trust cloud providers with their data. In large companies, this can be achieved by internal security departments, which would need to build the required competencies to assess and mitigate the risks. The SMEs may be unable to build such competencies internally.

Providers tend to regard the security issue as mainly a lack of security competence and skills among clients. In contrast, several articles and industry reports have documented that cloud computing does imply specific risks on the provider side, due to shared technology vulnerabilities, providers' unwillingness to disclose full details about security practices, and the sheer number of interactions between risks and challenges (Cloud Security Alliance, 2013; Khorshed, Ali, & Wasimi, 2012). According to John Howie (senior director of IT Security Services, Microsoft), the threat landscape is evolving, and their department has a threat team that is surveying evolving threats and modifying their controls in a continuous process (InfoQ.com, 2011). The Cloud Security Alliance (2010) has specified the top seven threats to cloud computing: *abuse and nefarious use of cloud computing; insecure APIs; malicious insiders; shared technology vulnerabilities; data loss/leakage; account, service, and traffic hijacking;* and *unknown risk profile*. We

conjecture that the security threats from the provider side are still present. Thus, there is a need for security audits of the providers and transparency regarding their security practices and audit reports. Such measures will be important to build trust in service providers.

Second, we note the prominence of strategy issues in the provider subpanel, and this is corroborated in the interviews. One significant issue is the need for contingency plans for incidents, in terms of dealing with both service interruptions and plans for migrating to another service provider. This requires a certain level of competence and maturity from the client.

Client maturity, in terms of the enterprise architecture and the ability to integrate cloud services in an appropriate manner, is an essential prerequisite to realize the potential benefits. Our study reveals that few clients have the appropriate competence and maturity levels. Moreover, most panelists overall perceive the cloud technology as still immature and difficult to integrate with the internal IT infrastructure.

Third, we recognize that legal issues are crucial, particularly data protection legislation. Countries have very different privacy and data protection laws (Greengard, 2012, p. 21). The issue of national and international data protection legislation has also been discussed in the literature (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011; Schneider & Sunyaev, 2014) and has been found to impede the adoption of cloud computing (Iyer & Henderson, 2012). Some countries do not have the legislative frameworks for using cloud services in the public sector (Shin, 2013); other countries and regions (e.g., EU) have very strict data privacy policies and regulations that should be reviewed (Kshetri & Murugesan, 2013). Nonetheless, some policy issues need to be reflected in data protection laws (Svantesson & Clarke, 2010). Data protection legislation regarding data about the public is the major concern of the clients from the public sector.

We observe that traditional SLAs are not feasible for CSPs, who cannot provide guarantees for performance levels since it would be too expensive in case of an incident. Thus, SLAs in cloud computing are weaker than those in traditional IT outsourcing, contributing to the clients' increased perceptions of security risks and loss of control. The SLA aspect is not explicitly covered by Schneider and Sunyaev (2014) but is related to the vendor characteristics of "service capability" and "trustworthiness." This factor therefore needs to be further researched in the cloud-computing context of IT outsourcing.

In the literature, it is argued that data protection laws focus on having the data physically located in a certain country or region (Desai, 2013; Greengard, 2012), which does not fit the borderless nature of a cloud-computing model. Both providers and clients note that privacy laws are lagging behind the development in cloud computing, and there is a need for international laws and policies. The financial industry has achieved this, and it will be important for a wide adoption of cloud computing.

References

Amazon. (2011). What is AWS? Retrieved May 20, 2011, from http://aws.amazon.com/what-is-aws/

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, D. R., & Konwinski, A. e. a. (2009). *Above the clouds: A Berkeley view of Cloud Computing*. Los Angeles: UC Berkeley Reliable Adaptive Distributed Systems Laboratory.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., . . . Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM, 53*(4), 50-58.

Avrane-Chopard, J., Borgault, T., & Moodley, L. (2014). Big Business in Small Business : Cloud Services for SMBs. *RECALL, McKinseyCompany, March 2014*.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599-616. doi: 10.1016/j.future.2008.12.001

Cloud Security Alliance, C. S. A. (2010). Top Threats to Cloud Computing. Retrieved Feb 20, 2015, from https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance, C. S. A. (2013). The Notorious Nine Cloud Computing Top Threats in 2013. Retrieved Feb 20, 2015, from https://cloudsecurityalliance.org/media/news/cloudbyte-measuring-and-mitigating-risk/

Desai, D. (2013). Beyond location: data security in the 21 st century. *Communications of the ACM, 56*(1), 34-36.

Goodburn, M. A., & Hill, S. (2010). The Cloud Transforms Business. *Financial Executive, 26*(10), 34-39.

Greengard, S. (2012). On the digital trail. *Communications of the ACM, 55*(11), 19-21.

Hsu, C.-C., & Sandford, B. A. (2007). The Delphi technique: making sense of consensus. *Practical assessment, research & evaluation, 12*(10), 1-8.

InfoQ.com. (2011). Cloud Computing Roundtable. Retrieved Jan 14, 2015, from http://www.infoq.com/articles/ieee-cloud-computing

Iyer, B., & Henderson, J. C. (2012). Business value from clouds: learning from users. *MIS Quarterly Executive, 11*(1), 51-60.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, 21-25 Sept. 2009). *On Technical Security Issues in Cloud Computing.* Paper presented at the Cloud Computing, 2009. CLOUD '09. IEEE International Conference on.

Khorshed, M. T., Ali, A. B. M. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems, 28*(6), 833-851. doi: http://dx.doi.org/10.1016/j.future.2012.01.006

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy, 37*(4), 372-386.

Kshetri, N., & Murugesan, S. (2013). Cloud computing and EU data privacy regulations. *Computer*(3), 86-89.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems, 51*(1), 176-189.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute of Standards and Technology. from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

Microsoft. (2011). Windows Azure. Retrieved June 22, 2011, from http://search.microsoft.com/results.aspx?form=MSHOME&mkt=en-us&setlang=en-us&q=Azure

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*(1), 15-29.

Pettey, C., & Stevens, H. (2009). Gartner says Cloud application infrastructure technologies need seven years to mature. Retrieved 4th February, 2011, from www.Gartner.com: http://www.gartner.com/it/page.jsp?id=871113

Salesforce. (2015). What is cloud computing? Retrieved Feb 12, 2015, from http://www.salesforce.com/eu/cloudcomputing/?fromSearch=true

Saya, S., Pee, L. G., & Kankanhalli, A. (2010). *THE IMPACT OF INSTITUTIONAL INFLUENCES ON PERCEIVED TECHNOLOGICAL CHARACTERISTICS AND REAL OPTIONS IN CLOUD COMPUTING ADOPTION.* Paper presented at the ICIS 2010 Proceedings, Paper 24.

Schmidt, R. C. (1997). Managing Delphi surveys using nonparametric statistical techniques*. *Decision Sciences, 28*(3), 763-774.

Schneider, S., & Sunyaev, A. (2014). Determinant factors of cloud-sourcing decisions: reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology*.

Shin, D.-H. (2013). User centric cloud service model in public sectors: Policy implications of cloud services. *Government Information Quarterly, 30*(2), 194-203.

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management, 31*(3), 272-278. doi: 10.1016/j.ijinfomgt.2010.08.001

Svantesson, D., & Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review, 26*(4), 391-397.

Vmware. (2011). Cloud Computing in Europe: Transformation is in the Air. *Market Pulse.* Retrieved June 22, 2011, from http://tibmek.nl/wp-content/uploads/2011/06/Cloud_FINAL_IDG_EMEA_Paper_EN.pdf

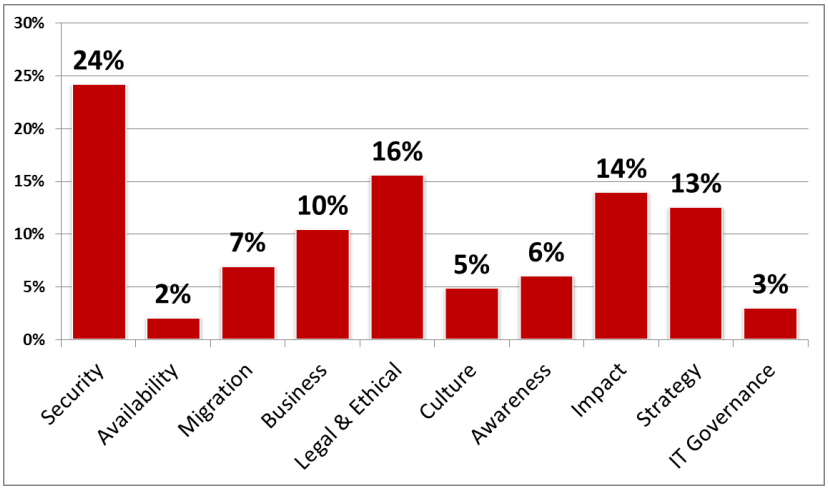
Vouk. (2004). Cloud computing–Issues, research and implementations. *Cit Journal of Computing and Information Technology, 16*(4), 235-246.

Xledger.net. (2015). Xledger.net - den mest omfattende ERP-løsningen i nettskyen. Retrieved March 10, 2015, from http://www.xledger.no/

7. Appendix 1

7.1 Detailed results from the brainstorming phase

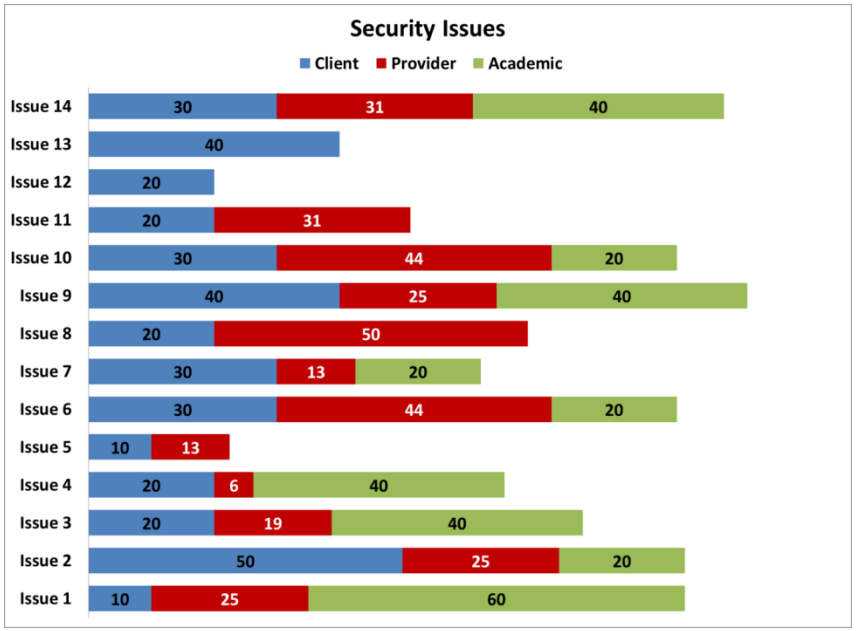
In the brainstorming phase, a list of 55 cloud computing adoption issues was generated and grouped into 10 categories. In the next stage, these issues were narrowed down to a list of 33 issues. The experts selected the issues they considered most important (10 to 20 issues were selected for each expert). The security category obtained 24% of the votes, followed by the legal and ethical category at 16%, the impact category at 14%, and the strategy category at 13%.



Category	Total votes
Security	104
Availability	9
Migration	30
Business	45
Legal & Ethical	67
Culture	21
Awareness	26
Impact	60
Strategy	54
IT Governance	13

7.1.1 Security issues

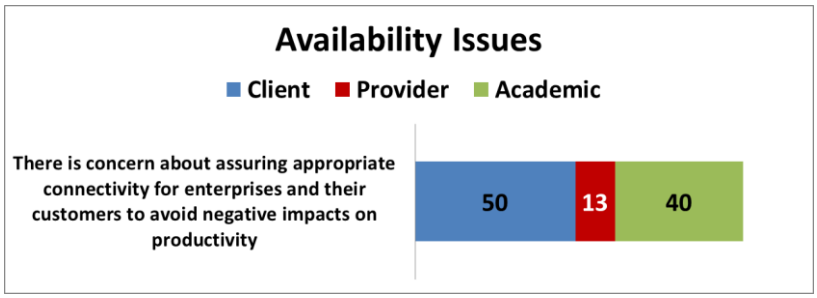
The percentage of votes from each subpanel is presented per security issue to understand the level of security issues in detail. The client subpanel gave issue2 the highest votes within the security category (50%). The provider subpanel voted issue8 as most important (50%), whereas the academic subpanel considered issue1 to be most important (60%).



Issue 1	Using public cloud services (bring your own cloud [BYOC]) for project collaboration may threaten employees' personal data and confidential business data. This also makes it difficult to maintain and control a security policy for access to and distribution of corporate information.
Issue 2	The risk of moving the enterprises' customer data to the cloud leaves enterprises hesitant, either to let the data stay in-house or move to the cloud. However, this depends on the cloud providers and the agreements between them and the enterprises.
Issue 3	The risk of losing control over resources (data, software, hardware, and human resources) in private clouds is less than that of public clouds. However, risks are not absolute, and most of them can be addressed but not all of them.
Issue 4	It is unclear who owns the data
Issue 5	Malicious insiders (i.e., cloud provider's employees) may access the cloud servers and steal confidential data of the cloud users.
Issue 6	One provider's SaaS application can be based on another provider's PaaS solution that runs on another provider's IaaS offering, which adds another level of security risks. It also becomes difficult to trace whether or not legislation and internal security policies are met.
Issue 7	Many cloud providers claim their compliance with security standards, but enterprises want to make sure that this is relevant to the kind of security they are looking for.
Issue 8	There may be insufficient and inconsistent data encryption policies and practices.
Issue 9	There are real security risks related to data theft, hacking, virus attacks, and data corruption. Specifically, if the hypervisor layer becomes compromised, all virtual machines can be hacked or deleted. However, private and hybrid clouds offer more security than public clouds regarding these issues.
Issue 10	There is a lack of trust in the cloud's multitenancy architecture and the governments of the countries where the data are stored. Thus, data need to be encrypted to make it hard to use customer data in case of leakage.
Issue 11	There is concern about making the data lifecycle secure in all its phases (i.e., create, store, use, share, archive, and destroy). An insecure data lifecycle may lead to data leakage. Regarding data deletion, if the provider does not provide proof that its data-wiping technique prevents data recovery, this will put customer data (i.e., financial data, employee records, or medical records) at risk, causing confidentiality problems, thus affecting the enterprise's reputation.
Issue 12	Multiple tenants may disrupt services unintentionally, causing a denial of service (DoS) attack that makes services unavailable, which leads to losing customers.
Issue 13	Enterprises in a certain geographic location trust in or are forced by the government to deal with cloud providers within their area, whether they provide the best service or not. On the other hand, these providers might be using third-party providers to store the data.
Issue 14	The security department's involvement is important at every step of the migration, from requirements gathering to technical implementation, until the support cycle is in production and operational.

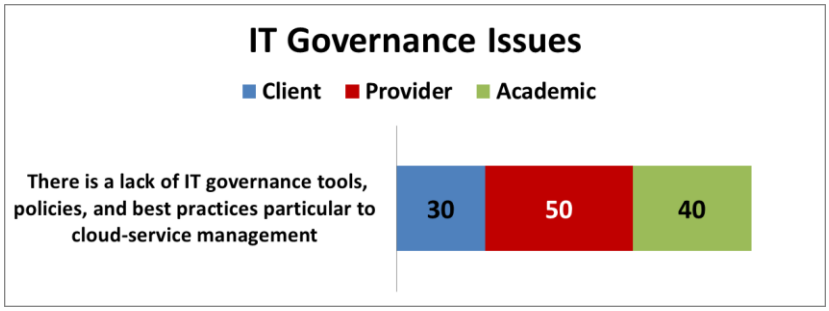
7.1.2 Availability issues

Cloud services are delivered over the Internet, so service availability poses a high concern for the client subpanel (50%). Similarly, the academic subpanel indicated the high importance of service availability (40%). The experts stated several causes of service unavailability, such as connectivity loss when providers upgrade network settings, digging into the ground, multi-tenant disruption causing denial-of-service attack, weak connectivity infrastructure in the country where the client organization is based, and performance degradation during the migration to the cloud environment.



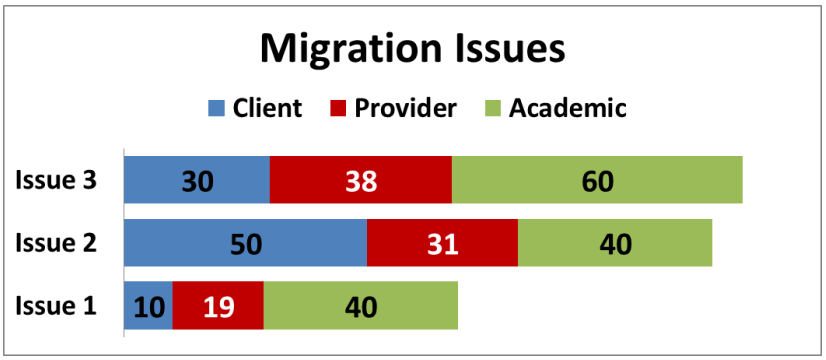
7.1.3 IT governance issues

IT governance gained the highest votes from the provider subpanel (50%) and the academic subpanel (40%). Some clients from highly regulated industries conduct regular audits related to their industry, and perhaps, they do not see any lack of IT governance tools or practices. However, providers seem to perceive that these governance practices are used to control the internal IT infrastructure and are not related to the cloud model in particular. An expert from the provider subpanel highlighted that organizations have IT governance practices to manage their own in-house IT infrastructure. Using cloud services will require adapting such internal governance practices to manage the external IT infrastructure operated by the cloud provider.



7.1.4 Migration issues

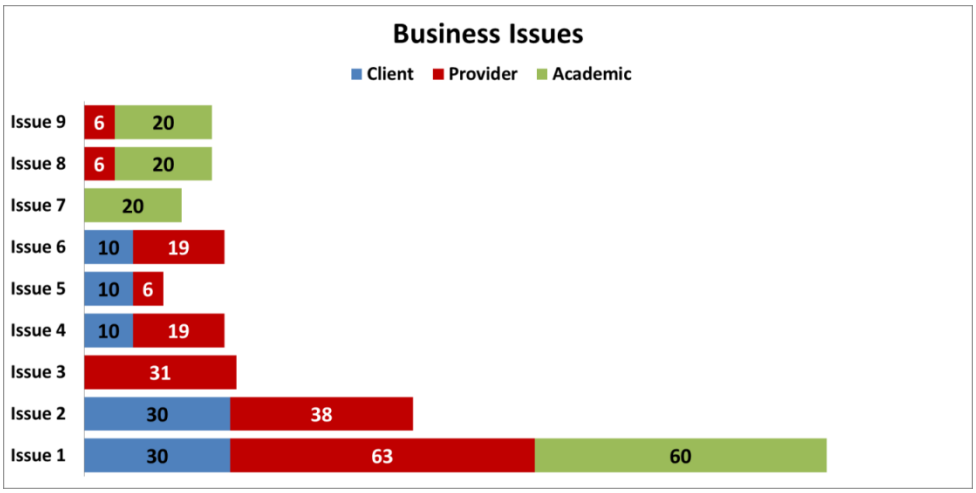
The client subpanel gave the highest votes (50%) to issue2. Most of the client organizations that participated in the study have subordinate business units that are spread nationally or internationally. An expert from the client subpanel said that a typical situation is that each business unit uses its own ITIL processes that need to be adapted to the cloud model (e.g., less support intervention, more automation, self-service, etc.) to become more mature at the technical level. Issue3 was voted the most by the provider subpanel (38%) and the academic subpanel (60%). One of the experts from the provider subpanel cited that migration experiences can either be poor or good. A poor migration happens when a client is unable to access the needed information for a certain task and receives no notice upfront. A good migration is fast, smooth, and efficient.



Issue 1	Each team/department/organization adopts its own concept of a cloud, and it becomes difficult to migrate all the clouds into one big cloud.
Issue 2	The lack of uniform support models makes it complex to integrate cloud solutions with the legacy, on-premise IT infrastructure, as well as data from different sources, which costs effort and time and may affect applications' availability and data integrity.
Issue 3	There is a lock-in concern about taking back the data and software from one cloud vendor and transferring them to another if the service is unsatisfactory, without affecting business operations.

7.1.5 Business issues

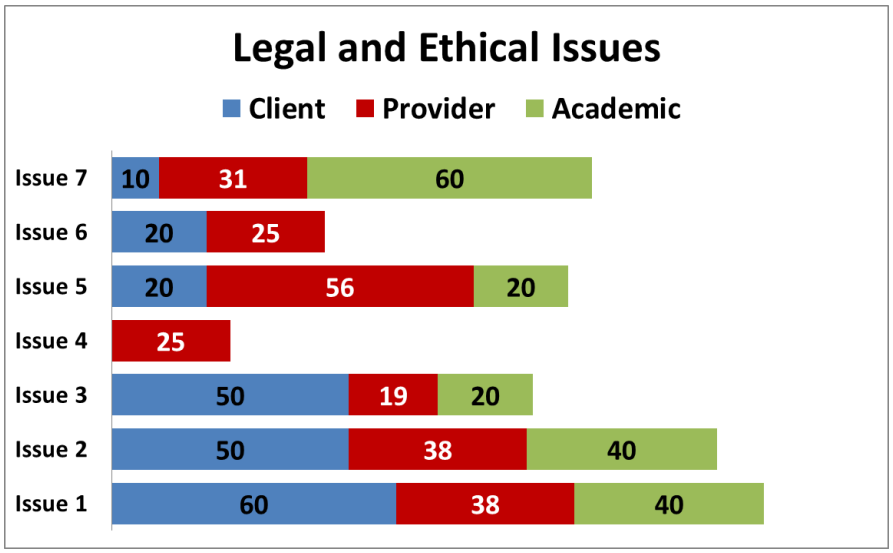
Issue1 and issue2 equally gained the most votes from the client subpanel (30%). Obviously, clients are taking a cost perspective toward the cloud computing model. Issue1 gained the most votes from both the provider subpanel (63%) and the academic subpanel (60%). Some providers indicated that clients often consider the cloud model mostly from a cost perspective. The providers see this as a wrong perspective to take when cloud services are adopted. For instance, public cloud services offer a flexible way of paying per use, but the services can be at the same cost level as on-premise solutions do. Cloud services should be considered from a business perspective to understand the business value that cloud services can bring to a client's enterprise. Thus, the providers emphasize that business needs should be the driving force for clients when cloud services are adopted.



Issue 1	If the cost of using cloud services is not lower than that of on-premise operations, it is difficult to obtain the management's support for the cloud strategy.
Issue 2	Despite the minimal investment costs of transferring to a cloud solution, organizations must expect a higher monthly rate.
Issue 3	The transition from capital expenditure to operational expenditure reduces operational margins but increases operational risks and could lead to a less predictable cost level.
Issue 4	Cloud solutions are difficult to sell because they are not supported by traditional sales models.
Issue 5	Cloud computing offers financial benefits and very well-articulated services but results in a higher total cost of ownership (TCO).
Issue 6	Budget constraints may lead to delays in implementing current visions. It has to be clear to the top management how much money can be saved in the future when spending so much at once.
Issue 7	There is fear of losing business and long-term brand recognition.
Issue 8	The slow development of suitable standards causes the lack of technological innovation within the cloud industry.
Issue 9	A significant amount of negative marketing exists in cloud services.

7.1.6 Legal and ethical issues

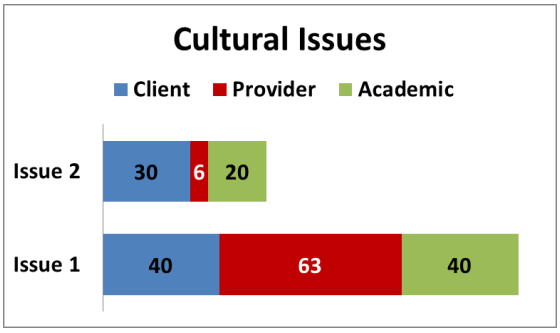
Issue1 gained the most votes (60%) from the client subpanel, which seemed to be highly concerned about this issue. In particular, this is the case for clients that are large enterprises, which connect their dispersed business through cloud solutions. They need to deal with conflicts because of local regulations that differ across countries. Issue5 gained the most votes from the provider subpanel (56%). Providers can understand that clients become confused because cloud providers do not use traditional SLAs. Good negotiation skills are needed to reach an acceptable agreement, and not all clients may have these skills. The academic subpanel gave the most votes to issue7 (60%); small and non-public sector clients may not have the competence and power to modify the agreements offered by international cloud providers.



Issue 1	Data protection legislation is different and not strong in all countries.
Issue 2	Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.
Issue 3	It is difficult for companies to get an overview of laws and standards, which make compliance a complicated issue and lead to applying traditional regulatory compliance that does not cover all cloud-computing aspects.
Issue 4	Standardized cloud-process models do not support customization, and organizations may have to change their processes and practices to maximize the benefits.
Issue 5	Enterprises are faced with weak, undetailed service level agreements (SLAs) from providers (e.g., providers may not be transparent about where and how they store the data and the acknowledgment of security incidents whenever they happen and how the cloud providers deal with them).
Issue 6	There is no standard service level agreement (SLA) for cloud-computing delivery methods due to unsolved security and environmental (such as supplier dependency) issues, which will lead to unclear segregation of duties between the cloud provider and the consumer (due to the lack of legal precedents) regarding responsibilities for personal and sensitive business data at the level of the service models, IaaS, PaaS, and SaaS). This raises potential security vulnerabilities.
Issue 7	It is hard for small clients to modify the standard agreements of major international cloud providers.

7.1.7 Cultural issues

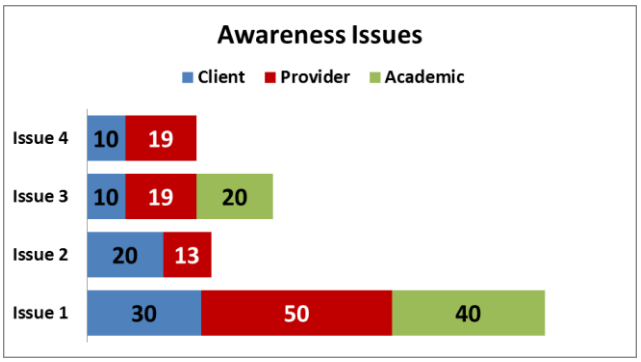
Issue1 gained the highest votes from the three subpanels at 40% for the client subpanel, 63% for the provider subpanel, and 40% for the academic subpanel. Old routines are a part of the corporate culture in companies, and they can cause resistance to change when new technical solutions are adopted. Enterprises need to carefully consider this issue.



Issue 1	People used to old systems will have to change how they work (more automation, less paperwork, new routines, etc.), which is hard for many people and should not be underestimated.
Issue 2	Some key people in the organization are powerful, and management may fear confronting them with change if they strongly oppose it.

7.1.8 Awareness issues

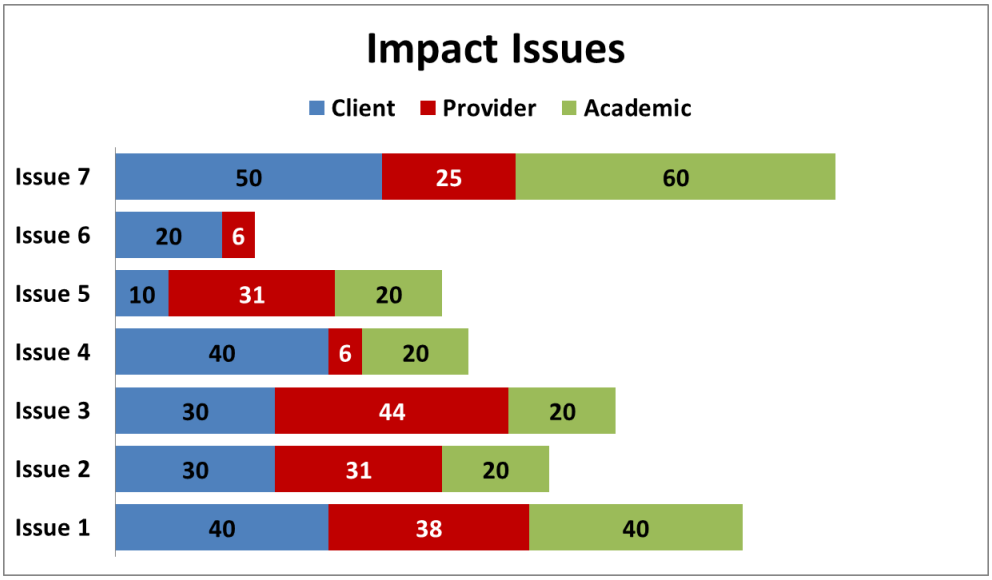
Obviously, issue1 gained the most votes from the three subpanels at 30% for the client subpanel, 50% for the provider subpanel, and 40% for the academic subpanel. Providers voted the most for issue1 because they experience it with some clients. These clients are often unaware of the potential business value that cloud services can add to their business because the meaning of the cloud concept is unclear to them.



Issue 1	The meaning of the cloud, the difference between it and on-premise, and the consequences of using it are unclear for the users (including managers), which may weaken its value.
Issue 2	There is reluctance to adopt a cloud service with less functionality or reduced user experience (efficiency and flexibility) than that of traditional solutions.
Issue 3	The consumer's lack of security awareness results in misuse of the cloud environment and misconfiguration of the cloud-environment layers.
Issue 4	There is a lack of analysis and sales activities as some vendors deliver IaaS as though it should be a pure public cloud. However, when clients more closely examine how vendors deliver their services, these do not fulfill customer expectations (some services are not automatically created, which cost effort and money to create) and turn out to be more like traditional outsourcing that is packed as a cloud service, sales wise.

7.1.9 Impact issues

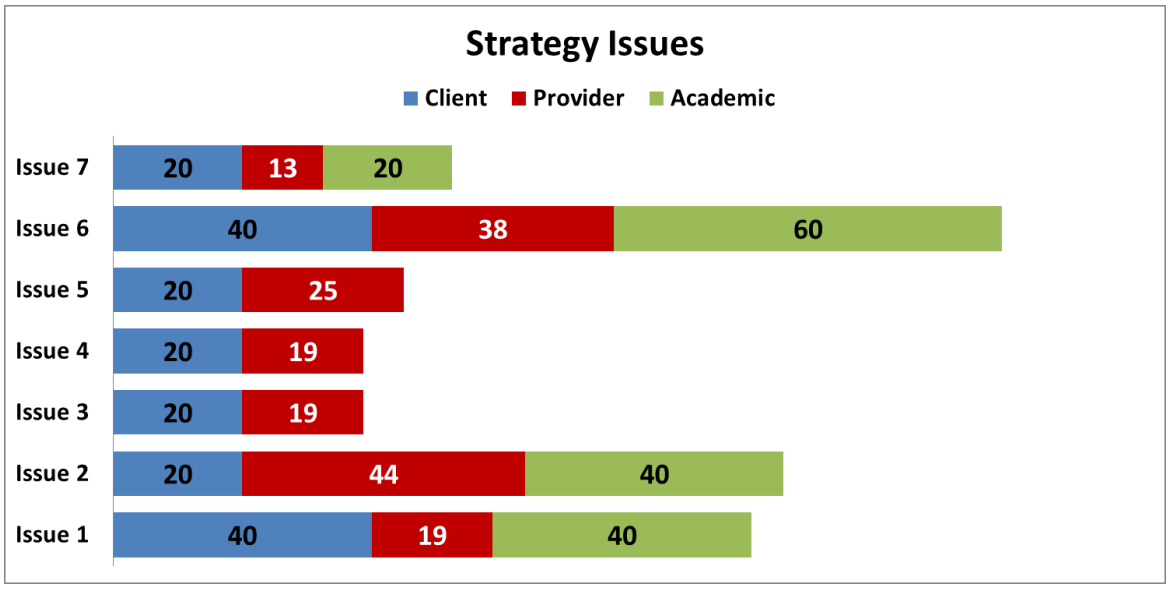
The client subpanel gave the most votes (50%) to issue7 because it is dependent on cloud providers in solving technical problems. Similarly, the academic subpanel gave most of its votes to issue7 (60%). The provider subpanel gave the most votes to issue3 (44%) because it asserts that clients need to adapt to the cloud business model in order to achieve the benefits of cloud services.



Issue 1	Implementing cloud services in organizations requires different skills and knowledge to control IT resources through SLAs (e.g., IT service management and negotiation with cloud providers), which can be expensive and time-consuming, especially in implementing private clouds.
Issue 2	User support is a critical component in building trust between business operations and IT services.
Issue 3	Organizations may fail to modify their business processes to leverage the effect of cloud-computing agility on business models.
Issue 4	There is concern about whether the transition to the cloud disturbs current IT and business operations.
Issue 5	Cloud computing offers an opportunity for reorganizing the IT department (laying off dedicated staff).
Issue 6	Maintaining an old organizational chart will lead to gaps in understanding new requirements from all involved teams.
Issue 7	The company depends on external routines and competence; if something happens, the enterprise cannot solve the issue itself and will be unable to perform its normal functions.

7.1.10 Strategy issues

The client subpanel gave an equally high importance to issue1 (40%) regarding the maturity of cloud service models, as well as issue6 (40%) regarding the need for recovery plans to keep the business running. The provider subpanel gave high importance to issue2 (44%) because it experienced lack of agreement across the departments of its clients' organizations. The academic subpanel also indicated the importance of recovery plans in issue6 (60%).



Issue 1	It is important to adopt cloud-service models that have a degree of maturity so that sensitive data and functions can be implemented in a private cloud; otherwise, it *must* be kept on-premise. On the other hand, nonsensitive data and functions can be outsourced to the cloud.
Issue 2	The failure to reach an agreement about the cloud-adoption strategy at all levels can stifle the best-intended initiative.
Issue 3	There is a huge variance in the demands for each organization/department/employee. Thus, the chosen model(s) have to serve all needs in the most efficient way compared to the traditional methods.
Issue 4	In many cases, the adoption is more "random," and the benefits disappear because key considerations are overlooked (in terms of what organizations actually want, what they expect, why they want to adopt the cloud, what can be implemented in the cloud, and how to transition).
Issue 5	Each organization is required to describe its enterprise architecture in detail to easily contract the correct cloud services for the "to-be" architecture.
Issue 6	Plans for dealing with incidents (downtime, provider goes bankrupt, or the data center is destroyed) should be in place to maintain business-critical operations.
Issue 7	It is important to evaluate the provider (in terms of experience with the industry, ability to provide advice on "cloud orchestration," operational stability, and long-term commitment) and ensure that prices are comparable across different vendors.

Examples of Data Analysis

Rankings from the Delphi study → **High priority (among the top 10)**

Issues (Legal and Ethical)	Client rankings	Provider rankings	Academic rankings
Data protection legislation is different and not strong in all countries.	1	10	3
Compliance with data privacy acts is mandatory, and it may slow down investing in and exploiting the full benefits of cloud services.	5	11	4

Evidence from the case of Norway

Code: Coercive pressure →

Datatilsynet banned the use of Google Apps in Narvik after finding that Google's data processor agreement did not fulfil information security requirements, according to the Norwegian law, regarding the location of the data, and Narvik did not conduct proper risk assessments (Veum & Thoreid 2012; Thon & Vetland 2012; Gould 2012). Datatilsynet had a concern about the U.S. Patriot Act and required Narvik to conduct risk assessment to get more information about data location, data segregation, and access controls (Gould 2012).

→ Re-interpreted as: **Banning**

Code: Strict regulations →

"our processes are written up into the national laws and regulations which regulate specialist healthcare in Norway....There is an opening to utilize cloud services that can document that they are localized in the EU, but I know, specifically, that we have tried to utilize cloud services, for example, from India and that has not been allowed…..so the laws regarding security of information about citizens are very very strict."

Client C4

"Norway is regulated by the central authority [Datatilsynet] for how the data are stored and confidentiality must be granted when the data are stored somewhere…. And the responsibility of the data is always the main issue where it is located…. If the data are stored outside the EU, then that is an issue because the EU has common regulations about how to protect the data not to let it outside of the community."

Client C11

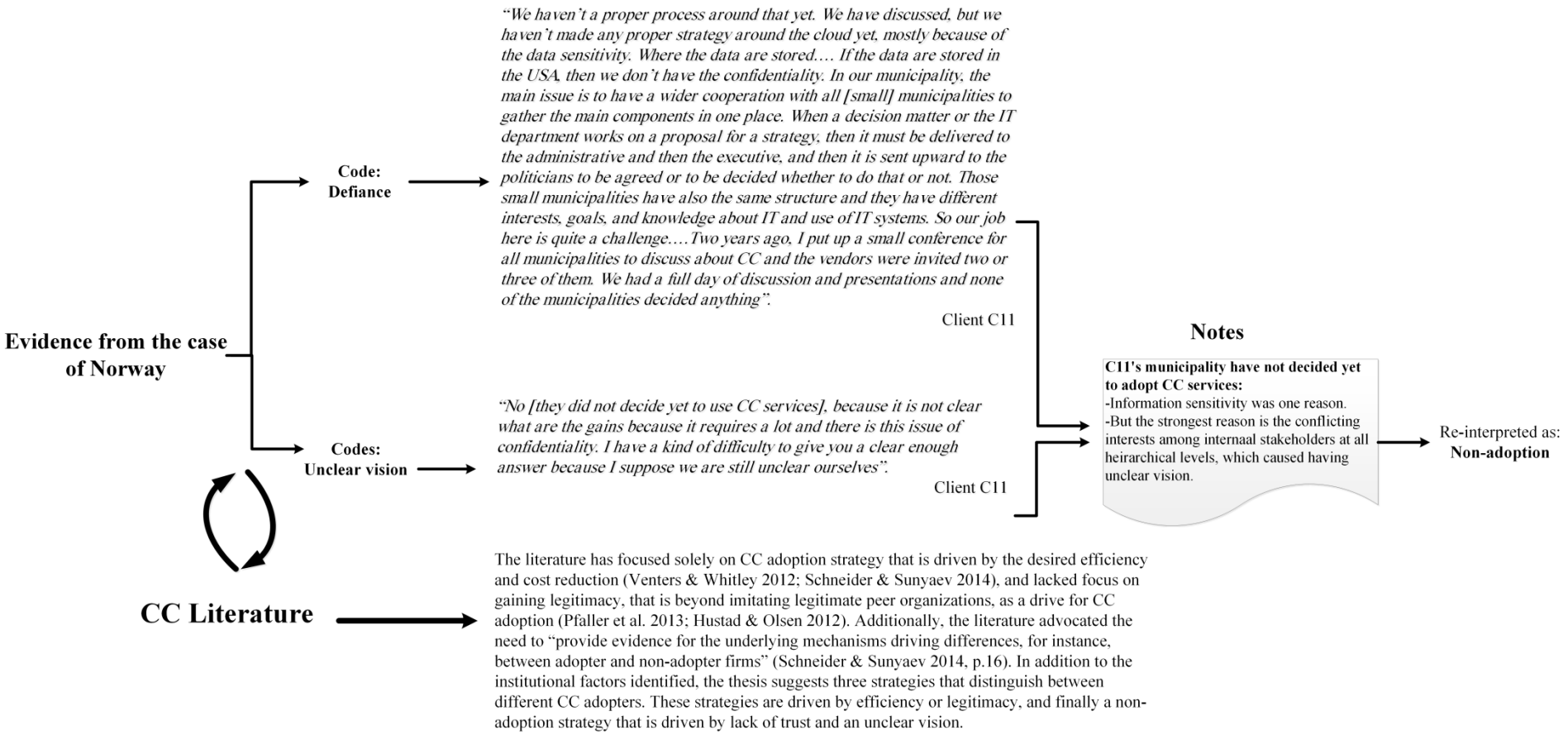
Resulted from →

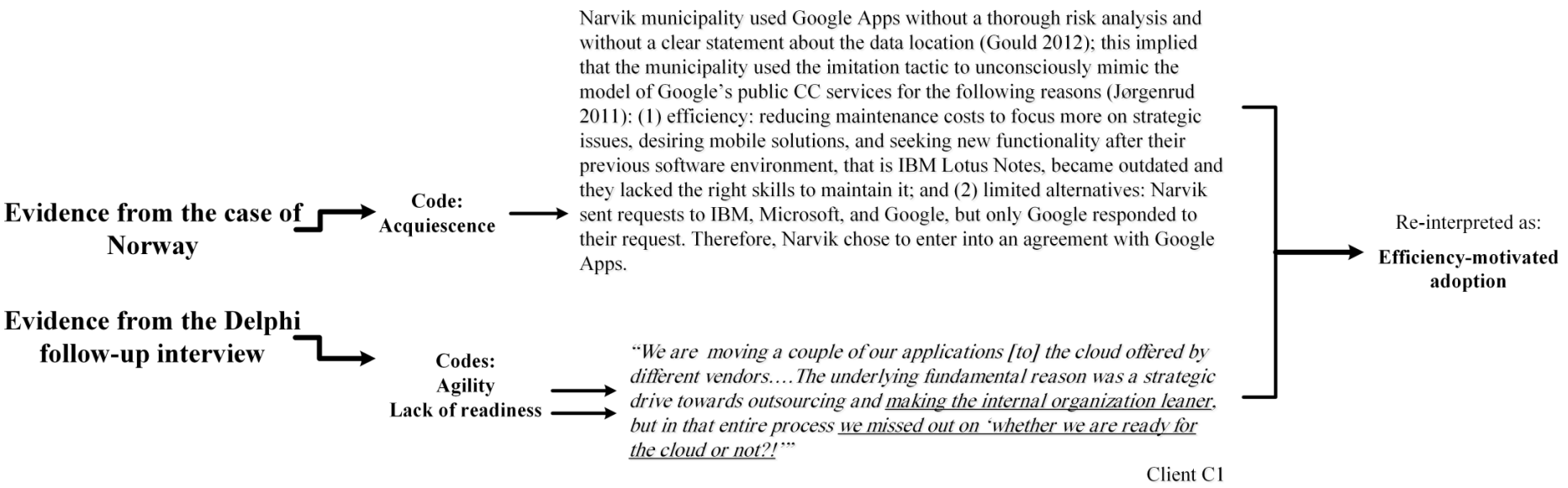
Code: Coercive pressure

"(1) that you [as a municipality] have to do, and it is required by the Norwegian law, risk analyses [before moving to the cloud]; (2) you have to have an agreement [called databehandleravtale] with the cloud service provider with specific needs according to the Norwegian law. So you cannot use the agreement directly from Microsoft…and Microsoft knows about it…and if you tell them that I cannot use your agreement because it is not according to the Norwegian law, so I have another agreement for you. They will say ok, it is fine, we know about it! So, you just come with your agreement and this agreement should you use is on the pages of Datatilsynet's home pages; (3) then you actually are required by the law to implement regular security audits of Microsoft if you choose Microsoft, and of Google if you choose Google. So Moss and Narvik, they now get information about security audits on Microsoft and Google. You need to get that information and you need to have those documents stored in your house to be according with the Norwegian law".

Provider P16

→ Re-interpreted as: **Regulations and guidelines**


Evidence from the case of Norway
Code: Defiance
"We haven't a proper process around that yet. We have discussed, but we haven't made any proper strategy around the cloud yet, mostly because of the data sensitivity. Where the data are stored.… If the data are stored in the USA, then we don't have the confidentiality. In our municipality, the main issue is to have a wider cooperation with all [small] municipalities to gather the main components in one place. When a decision matter or the IT department works on a proposal for a strategy, then it must be delivered to the administrative and then the executive, and then it is sent upward to the politicians to be agreed or to be decided whether to do that or not. Those small municipalities have also the same structure and they have different interests, goals, and knowledge about IT and use of IT systems. So our job here is quite a challenge.…Two years ago, I put up a small conference for all municipalities to discuss about CC and the vendors were invited two or three of them. We had a full day of discussion and presentations and none of the municipalities decided anything".
Client C11
Codes: Unclear vision
"No [they did not decide yet to use CC services], because it is not clear what are the gains because it requires a lot and there is this issue of confidentiality. I have a kind of difficulty to give you a clear enough answer because I suppose we are still unclear ourselves".
Client C11
Notes
C11's municipality have not decided yet to adopt CC services:
-Information sensitivity was one reason.
-But the strongest reason is the conflicting interests among internaal stakeholders at all heirarchical levels, which caused having unclear vision.
Re-interpreted as:
Non-adoption
CC Literature
The literature has focused solely on CC adoption strategy that is driven by the desired efficiency and cost reduction (Venters & Whitley 2012; Schneider & Sunyaev 2014), and lacked focus on gaining legitimacy, that is beyond imitating legitimate peer organizations, as a drive for CC adoption (Pfaller et al. 2013; Hustad & Olsen 2012). Additionally, the literature advocated the need to "provide evidence for the underlying mechanisms driving differences, for instance, between adopter and non-adopter firms" (Schneider & Sunyaev 2014, p.16). In addition to the institutional factors identified, the thesis suggests three strategies that distinguish between different CC adopters. These strategies are driven by efficiency or legitimacy, and finally a non-adoption strategy that is driven by lack of trust and an unclear vision.


Evidence from the case of Norway
Code: Acquiescence
Narvik municipality used Google Apps without a thorough risk analysis and without a clear statement about the data location (Gould 2012); this implied that the municipality used the imitation tactic to unconsciously mimic the model of Google's public CC services for the following reasons (Jørgenrud 2011): (1) efficiency: reducing maintenance costs to focus more on strategic issues, desiring mobile solutions, and seeking new functionality after their previous software environment, that is IBM Lotus Notes, became outdated and they lacked the right skills to maintain it; and (2) limited alternatives: Narvik sent requests to IBM, Microsoft, and Google, but only Google responded to their request. Therefore, Narvik chose to enter into an agreement with Google Apps.
Evidence from the Delphi follow-up interview
Codes: Agility Lack of readiness
"We are moving a couple of our applications [to] the cloud offered by different vendors.…The underlying fundamental reason was a strategic drive towards outsourcing and making the internal organization leaner, but in that entire process we missed out on 'whether we are ready for the cloud or not?!'"
Client C1
Re-interpreted as:
Efficiency-motivated adoption