UNIVERSITY OF SOUTHAMPTON

FACULTY OF PHYSICAL AND APPLIED SCIENCES

Electronic and Computer Sciences

A Framework for the Implementation of a Private Government Cloud in Saudi Arabia

by

Amal Saleh Alkhlewi

Thesis for the degree of Doctor of Philosophy in Computer Science

April_2018

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF PHYSICAL AND APPLIED SCIENCES

Electronic and Computer Sciences

Thesis for the degree of Doctor of Philosophy in Computer Science

A FRAMEWORK FOR THE IMPLEMENTATION OF A PRIVATE GOVERNMENT CLOUD IN SAUDI ARABIA

Amal Saleh Alkhlewi

Despite the effort and copious resources Saudi Arabia is investing in its transition towards e-Government, it is hindered by the weakness of the Information and Communication Technology infrastructure in its government agencies. The development of a private government cloud is a solution for improving and standardizing the ICT infrastructure, but cloud computing is still in the early stages in the country. To effectively implement a private government cloud in Saudi Arabia it is necessary to identify the factors that will affect its success. Therefore, this research identifies the success factors for the implementation of a government cloud, and based on these factors, a framework for the successful implementation of a government cloud (FSIGC) in Saudi Arabia was developed. The framework was constructed by synthesizing factors identified from relevant studies concerned with the implementation of cloud computing for government and factors identified from studies concerned with the success of large scale IT projects in Saudi Arabia.

A mixed-method research approach was followed to improve and confirm the initial 10 factor framework which was developed from a literature review. The ten factors identified were: Security and Privacy, Reliability, Cooperation and Coordination, Policy and Legislation, Leadership, Business Process Re-Engineering (BPR), Project planning, Top management support, Consultant and

team competence, Clear requirements. First, interviews were carried out with twelve IT experts working in Saudi government organisations to review the proposed success factors and identify any additional factors not identified from the literature review. The expert review produced five additional factors to the ten proposed in the desk-based study: Communication, Standards, Training, Knowledge Management, Business continuity and disaster recovery. Next, an online survey of government IT employees was conducted to confirm the fifteen component framework. The results from the survey showed that all the factors in the framework were statistically significant.

The validated FSIGC framework was applied in the construction of a measurement instrument called the Government Cloud Readiness Measure. Initially, the instrument was developed by proposing scales to measure each of the factors in FSIG from a desk based study. Then, the instrument was confirmed and validated in two stages. First, an expert review was conducted to confirm its content validity and identify any additional items. Then, the instrument was confirmed by 11 experts and then tested for reliability through an online survey of 153 government and semi-government IT employees.

This research presents the detailed development of the FSIGC, its validation and application in the construction of the Government Cloud Readiness Measure. The findings of this study provide practical guidelines for government organisations in Saudi Arabia and other gulf countries to help increase the success of their cloud implementation projects, thus bridging the gap between theory and practice. This research can also be used as a starting point for other new technology implementation investigations in the public sector.

Table of Contents

List of tables

List of figures

DECLARATION OF AUTHORSHIP

I, Amal Saleh Alkhlewi, declare that this thesis and the work presented in it are my own and have been generated by me as the result of my own original research.

A Framework for the Implementation of a Private Government Cloud in Saudi Arabia

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:

Alkhlewi, A., Walters, R. J., & Wills, G. B. (2015). Factors Influencing the Implementation of a Private Government Cloud in Saudi Arabia. In ESaaSA@ CLOSER (pp. 69-72).

Alkhlewi, A., Walters, R., & Wills, G. (2015, August). Success factors for the implementation of a private government cloud in Saudi Arabia. In Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on (pp. 387-390). IEEE.

Alkhlewi, A., Walters, R. J., & Wills, G. B. (2019). Towards a Framework for the Successful Implementation of a Government Cloud in Saudi Arabia. International Journal of Business Process Integration and Management.

Signed: .....

Date: .....

Acknowledgements

I am grateful to Allah for blessing me with the opportunity to commence my research journey and providing me with the necessary faith and supportive network of family, friends and supervisors to complete it.

I would like to express my deepest appreciation to my wonderful supervisors Dr. Robert Walters and Dr. Gary Wills. Their support, guidance and kindness have made it possible for me to reach this point.

My family are the source my strength and achievements. They are always happy to provide any support that I need, be it proofreading, babysitting, prayers or just listening to my complaints. My sincere gratitude goes to my parents, Elizabeth and Saleh for always having faith in me; to my husband, Faisal, for his unwavering patience, support and positive attitude; to my siblings for always being willing to take time out of their lives to support me.

My children Albaraa, Khowla and Ubai have been my constant companions on this journey. Their constant calls of 'Are you done yet?!' have helped keep me on track. I would like to express my appreciation and pride for their patience, maturity and companionship.

I would like to thank my sponsor, Jubail University College, for sending me on this journey. I would also like to extend many thanks to all the IT experts and government employees that kindly took the time to answer my questions or complete a survey. Their data and input has been tremendously valuable to my research.

Last but not least, I would like to thank my friends for their support and encouragement.

Definitions and Abbreviations

BPR- Business Process Re-Engineering

CC- Cloud Computing

E-Government – Electronic Government

ERP – Enterprise Resource Planning

FSIGC- Framework for the Successful Implementation of a Government Cloud

G-Cloud – Government Cloud

G2C – Government to Citizen Interaction

G2B – Government to Business Interaction

G2E – Government to Employee Interaction

G2G – Government to Government Interaction

ICT – Information and Communication Technology

KSA – Kingdom of Saudi Arabia

NIST – National Institute of Standards and Technology

CSF- Critical Success Factor

IS- Information Systems

Chapter 1: Introduction

An introduction to the current research is given in this chapter. It commences with explaining motivation for the research and the problem it attempts to solve in section 1.1. Then, the major aims and objectives for the research are highlighted in section 1.2. Following that, the research questions that are answered in this study are listed in section 1.3. Finally, the chapter concludes with an overview of the thesis structure in section 1.4.

1.1 Motivation for the Research

The use of ICT by governments to provide more efficient and effective services to citizens is increasing worldwide (Ndou, 2004). The function of e-government is to provide efficient government management of and access to information for citizens, thus enhancing service delivery (UN, 2014), however, many e-government initiatives in developing countries have failed (UN, 2005) due to technological barriers, lack of resources, cost, digital divide, poor management and infrastructure, and lack of IT infrastructure (Almarabeh, Majdalawi, &Mohammad, 2016) .

There is no universally accepted definition of e-government. While the United Nations defines e-government as *"the use of ICT and its application by the government for the provision of information and public services to the people*", Riad et al. (2010) proposes a more comprehensive definition: "E-government includes government activities that take place over electronic communications among all levels of government, citizens, and businesses to deliver products and services; placing and receiving orders; providing and obtaining information; and completing financial transactions" , and it is this definition that will be adopted for the purpose of this study.

There are four major forms of interaction in e-government:

- Between government and citizen (G2C)
- Between government and business (G2B)
- Between government and employee (G2E)
- Between government department and government department (G2G)

The Kingdom of Saudi Arabia is in the process of transitioning to e-government – a process which began in 2005. The program developed for this is called "Yesser", which means "simplify" in Arabic and the system's purpose is to simplify government transactions for citizens.

According to the Saudi eGovernment Program's website, the role of Yesser is "*enabling the implementation of e government*" (e-GovProgram, 2013). On its official website, The Saudi National Portal, the current e-Government Program goals are listed as: to raise the productivity and efficiency of the public sector; to provide better and easier to access services to individuals and businesses; to increase investment returns; and to provide required information with high accuracy in a timely manner.

Since it commenced, Yesser has had two consecutive action plans (Yesser, Yesser Anual Report, 2011) (Yesser, 2014) as set out in the initial Saudi government strategy: The objectives of the First Action Plan (2006 -2010) were to "*deliver all possible official intra-governmental communication in a paperless way*", and to "*ensure accessibility of all information needed across government agencies and storage of information with as little redundancy as possible*" (e-GovProgram, 2013). The original vision statement of the program promised fully implemented e-government services throughout the Kingdom, however, by 2010, only 24% of the planned services were fully available, 8% were partially available, 29% were under development and 39% had not even started development (Franke & Eckhardt, 2014). When reporting on the first action plan in 2011, the weak ICT infrastructure in government organisations was emphasized as a key issue faced by the program (Yesser, 2011). The second action plan began in 2012 with a completion deadline of 2016 (Gov, 2012); however, to date no reports on the second action plan have been published, and a 3rd Action Plan is currently being prepared (Alfayad & Abbott-Halpin, 2017).

In their 2014 study of Yesser, Frank & Eckhardt found that the Saudi e-government program had not yet reached its full potential. Others found that Yesser is facing several challenges and obstacles which impede its implementation, including infrastructural, cultural and systemic factors (Alfarraj, et al., 2013) (Aldraehim, et al., 2012) (Alshehri, et al., 2012). Al-Nuaim (2011) notes that while the Saudi government has the necessary assets to fund e-government, implementation is impeded by the slow growth of government

services. Alshehri et al. (2012) noted several "systemic barriers to e-Government in Saudi Arabia, including IT infrastructural weakness in government sector, lack of public knowledge about e-Government, lack of systems to provide security and privacy of information, and lack of qualified IT and government service expert personnel". Alfarraj et al. (2013) noted that the Yesser e-Government program had changed its vision from offering electronic services to supporting the infrastructure projects, particularly of government organizations, citing weakness in the public sectors infrastructure as a justification for the change.

One proposed contributing factor to the difficulties faced is that the different government agencies in Saudi Arabia are at varying levels of ICT maturity which hinders the horizontal and vertical provision of e-government services (Alghamdi, et al., 2014). Alghamdi et al. (2014) found that ICT in Saudi Arabia is lacking in rural areas and there is insufficient integration among government organizations and their branches. A study published by Alassim et al. (2017) found that updating the technical infrastructure was still a major factor affecting Saudi Arabia's e-government efforts. They state that "*The infrastructure for the public sector does not seem to be equipped at this point in time to support the vision of Yesser*" (Alassim et al., 2017). On April 25th, 2016, Prince Mohammed Bin Salman announced a new long-term economic vision for Saudi Arabia named Vision 2030. One goal outlined in the plan is development of the kingdom's digital infrastructure. Technology will be a key enabler in Vision 2030's successful implementation for other goals, which include increased transparency, enhanced communication between government and citizens, increased government effectiveness and efficiency, and raising the kingdom]'s 2018 position as 54th in world ranking in the Government Effectiveness Index published by the World Bank to 20th or better by 2030 (Vision 2030). The 2018 E-Government Development Index (EGDI) which measures three important aspects of e-government; provision of online services, telecommunication connectivity and human capacity development gave Saudi Arabia a rating of 0.7119% (UN E-Government Development Index , 2018).

Having a reliable technical infrastructure is a precursor for Yesser to succeed (Alfayad & Abbott-Halpin, 2017). Cloud computing can be used to help governments quickly develop and strengthen their ICT infrastructure (Wyld,

2009) (Khan, et al., 2011) (Tripathi & Parihar, 2011) (Zwattendorfer, et al., 2013). It allows governments to uniformly supply e-government services, irrespective of any variations in maturity levels in different government agencies (Tripathi & Parihar, 2011) which do exist amongst the various Saudi government agencies . Many countries have begun to recognize the benefits of utilizing cloud computing in government (Hodgkinson, 2012). In Europe, the leading utilization method is to develop a G-Cloud, which is usually in the form of a private cloud that provides government services within the country (Zwattendorfer, et al., 2013). Asthe effectiveness of government clouds is improved when they are established in their own countries (Yeh et al., 2010), the development of a private government cloud could support Saudi Arabia in achieving its e-government targets. The aim of this research is to explore the factors that will facilitate the successful implementation of a private government cloud in Saudi Arabia. The aims and objectives for this research are explained in the following sections.

1.2 Research Aims and Objectives

The aim of this research is to identify the factors affecting the successful implementation of a private government cloud in Saudi Arabia and to assess government's readiness to implement a private cloud. To this aim the objectives for the study are the following:

- To identify the factors that might affect successful implementation of a private government cloud.
- To develop a framework that will aid the public sector in implementing a private cloud.
- To provide the public sector with an instrument to assess its readiness for implementing a private cloud.
- To help the public sector increase its readiness for implementing a private cloud.

1.3 Research Questions

The research questions asked and answered in this study are:

1) What framework will lead to the successful implementation of a private government cloud in Saudi Arabia?

a. What are the factors affecting the successful implementation of a private government cloud in Saudi Arabia?
b. How can these factors be validated?

2) Are Saudi government agencies ready to implement a private government cloud?
   a. What is a possible instrument that can be used to assess the level cloud implementation readiness?
   b. How can the instrument be validated?
   c. What is the cloud readiness score for Saudi government agencies?

1.4 Thesis Structure

This thesis is structured as follows (see Figure 1):

Chapter two: Sets the background for this study by describing the concepts and principals of cloud computing. Then, it reviews relevant literature to identify possible factors affecting the implementation of a private government cloud in Saudi Arabia. To this end, factors affecting both government cloud projects in general and Saudi government IT projects specifically were explored.

Chapter three: Describes the proposed framework for the successful implementation of a private government cloud and its components which was developed by synthesising the factors identified in the literature review.

Chapter four: Highlights the research methods used in the study and the rationale behind the choice of a triangulated mixed research method which includes semi-structured interviews with twelve IT experts from Saudi government agencies and an online survey of thirty IT experts from Saudi government agencies, after which the results of the semi-structured interviews and online survey are presented. The positive results from this study showed that the success factors in the framework are theoretically sound and ready for further applications.

Chapter five: Describes how the framework was applied in the development of an instrument for measuring the readiness of Saudi Arabian government agencies to implement cloud computing.

Chapter six: Details the confirmation and validation of the proposed instrument; eleven experts reviewed and confirmed the instrument, followed by a survey of a sample of 153 government IT employees to statistically validate the instrument.

Chapter seven: Concludes this research, highlights the contributions made during the course of this study, and outlines avenues for future research.

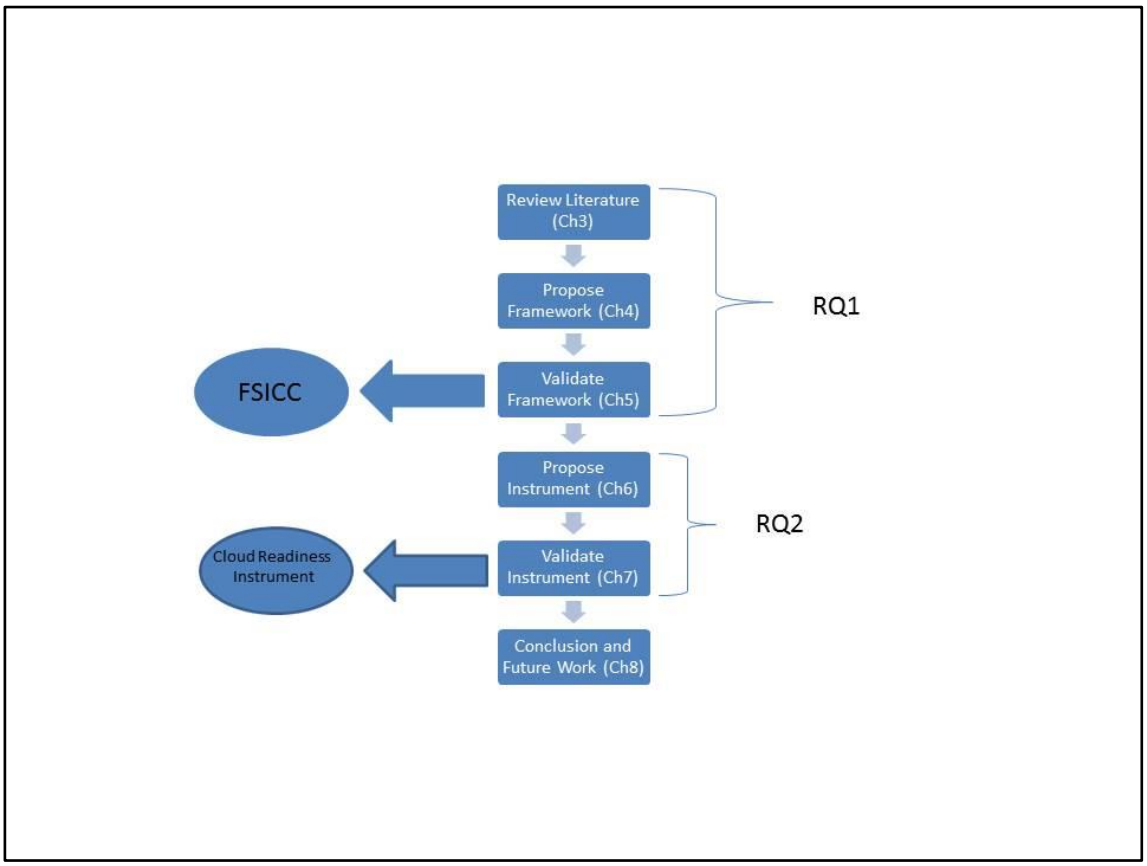

Figure 1 Thesis Overview

Chapter 2: Literature Review

This chapter provides background context and a review of current literature for the study. It starts with an explanation of cloud computing and its categories and characteristics in 0 . In section 2.3current literature investigating cloud computing in the Saudi Arabian public sector are explored. Following that, challenges to the implementation of cloud computing in government are highlighted in section 2.4 and challenges faced by large scale government IT projects in Saudi Arabia in section 2.5. The chapter is summarised in section 2.6.

2.1 Cloud Computing

The European Commission (2010) defines a cloud as: "*an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)*". The U.S National Institute of Standards and Technology (NIST) defines cloud computing 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). In the United States Federal Cloud Computing Strategy Kundra (2011) characterizes cloud computing as a:"…*profound economic and technical shift (with) great potential to reduce the cost of federal Information Technology (IT) systems while … improving IT capabilities and stimulating innovation in IT solutions* ". In the following subsections cloud computing is explained in more detail.

2.1.1 The Development of Cloud Computing

The theoretical possibility of cloud computing has been around for over 50 years. Cloud computing developed from several pre-existing computing technologies such as grid computing, utility computing, parallel computing, and virtualization, etc. Companies, such as Salesforce.com began selling their

software through a subscription rather than by licensing the user. However, this Software-as-a-Service (SaaS) model in which remotely hosted software could be accessed when and as needed for a fee did not offer any form of infrastructure. That came later, with the advent of Infrastructure-as-a- Service (SaaS) such as Amazon EC2 and S3, Rackspace, AT&T, and Verizon (Rajan & Shanmugapriyaa, 2012). Today there are a multitude of cloud services and hosting options that organizations can choose from. Gartner predict that enterprises will leverage their IT departments to take advantage of cloud computing's flexibility and cost saving benefits (Smith, 2017).

2.1.2 Types of Clouds and Service Models

NIST defines four Cloud deployment models -public, private, hybrid and community; classification is based on the scope of services offered to cloud customers. There are some common features in the four models including: resource distribution, accessibility through networks, and on-demand delivery (Géczy et al., 2012). The primary differences between the models lie in their scope and access (see Figure 2). A detailed comparison is give in Table 1. When adopting cloud computing for e-government both private and hybrid models have been used.

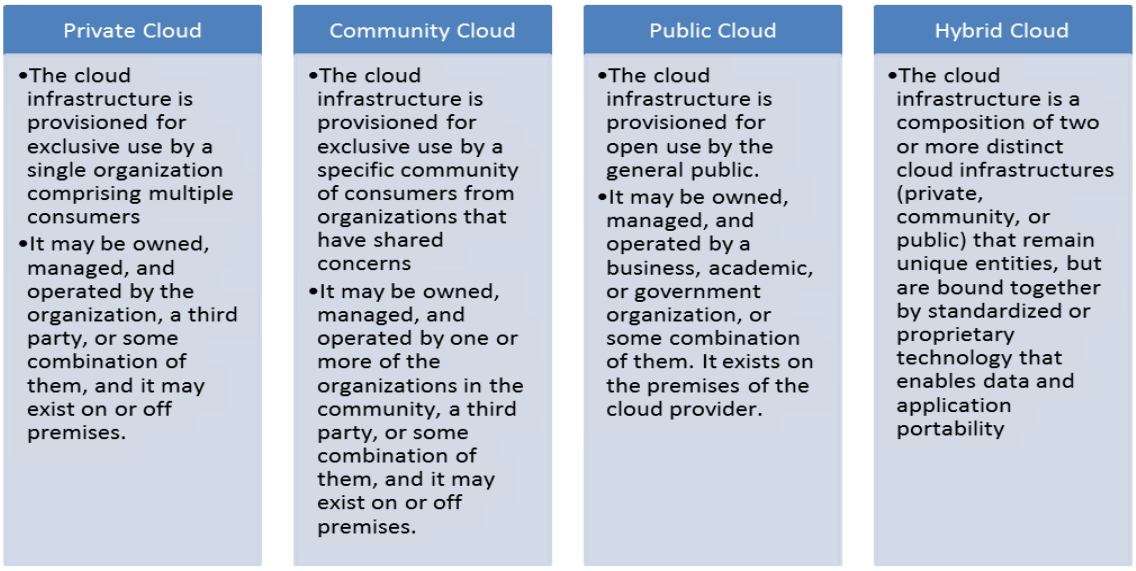

Figure 2 NIST Cloud Deployment Models

Table 1 Comparison of Cloud Deployment Models

Cloud Type	Public	Community	Private	Hybrid
Benefits	Ease of setup and use Easy access to data Capacity flexibility Low set up costs Scalability	More cost effective than public Improved security and privacy Increased reliability Ease of data sharing and collaboration	Control over Storage and network Scalability Architected to meet organization's specific needs Privacy High data security Reliability Lower operating cost Ease of integration with legacy system	Improved security and privacy in comparison to public and community clouds Enhanced scalability and flexibility Lower cost than private
Challenges	Data security and privacy Reliability Limitations in providing organization specific needs Hidden running costs	Cost in comparison to public cloud Shared storage and bandwidth capacity	High set up cost	Greater risk to data security than private
Type of organization applied by	Commercial organizations with fluctuating scalability requirements	Organizations with similar IT needs	Larger organizations with multiple department and with data security needs	Organizations that can separate between high and low security data
Examples		NYSE Capital Market Community Platform	Target, InterContinental Hotels Group,	NASA, Apple
Provider Examples	Dropbox , Google drive , Amazon Web services		VMware, Hewitt Packard Singapore's G-Cloud	

Mell & Gance (2011) provided three service models for cloud computing. Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud

Infrastructure as a Service (IaaS)). Others have included two additional service models: communications as a Service (CaaS) and Monitoring as a Service (MaaS) (Rittinghouse & Ransome, 2009). The service models differ depending on where the applications are deployed and whether they are managed on or off premises. Figure 3 explains the difference between cloud service models (Schouten, 2013).

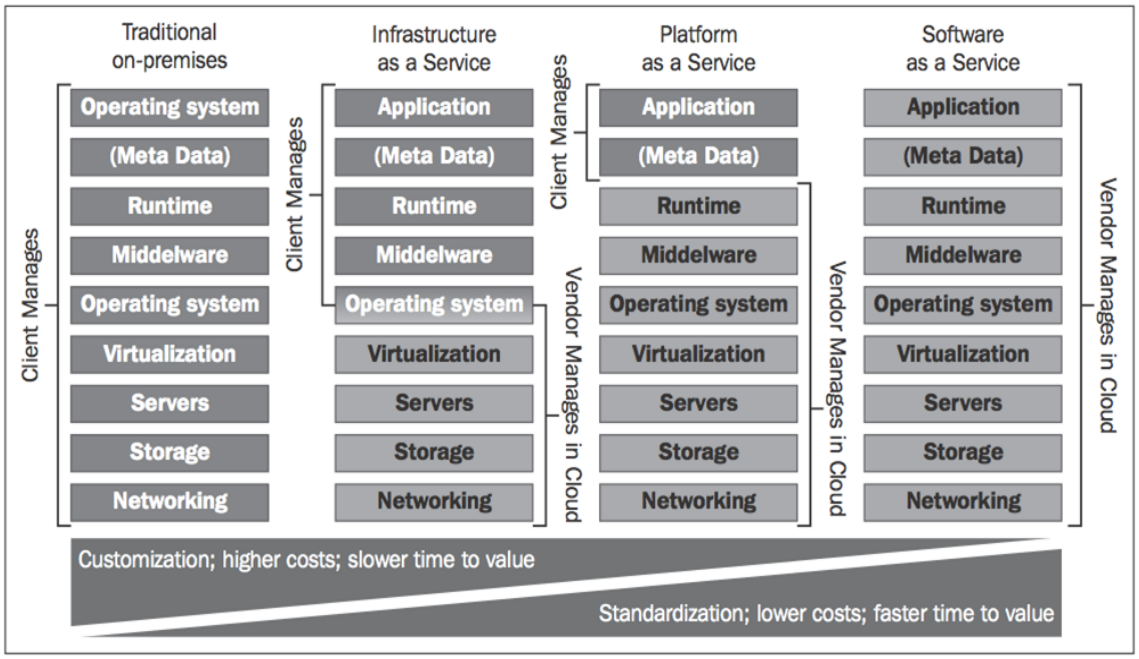

Figure 3 Cloud Service Models

The SaaS service model allows end users to gain access to applications on a pay-per-use basis (Chen et al., 2010). While, the PaaS service model allows end users to develop applications, tailored to their specific needs, but it does not give them control over the cloud infrastructure (Chen, Wills, Gilbert, & Bacigalupo, 2010). Alternatively, the IaaS service model provides end users with diverse resources, such as operating systems, storage, networking and databases; the end user can control these resources, but not the cloud infrastructure (Mell and Grance, 2009; Chen et al., 2010). So, IaaS allows for greater flexibility.

2.1.3 Characteristics of Clouds

Mell & Gance (2011) stated that cloud computing promotes availability, and proposed five essential characteristics of cloud computing: on-demand self-

service, broad network access, resource pooling, rapid elasticity, and measured service. According to Hodgkinson (2012) the key attributes of the cloud innovation are scale, focus, multi-tenancy, resilience, iterative evolution, use of SOA, social and mobile technologies, internet age security, self-service, usage-based charging, and vendor ecosystems. Buyya et al. (2011) describe cloud computing as a developing domain whose fundamental novelty resides in its characteristics of rapid elasticity for scaling an application when needed, and resource pooling to achieve higher utilization rates, lower costs, and a pay-as-you-go pricing model similar to a utility. (Lakshminarayanan et al., 2013) propose that using cloud computing will reduce the time IT staff spend on maintenance and update support.

2.2 Government Clouds

Hodgkinson (2012) proposed government demand for ICT enabled service provision is greater than available funding, resources and skills, proposing mature enterprise grade cloud services as a solution. Government clouds are seen as the new model for e-Government (Liang, 2012) (Hodgkinson, 2012). Wyld (2009) suggests that the value proposition of cloud computing has great appeal to governments due to the dynamic nature of IT demands and the challenging economic conditions many governments face. Cellary& Strykowski (2009) found that e-Government solutions should be created with cloud computing and service-oriented architecture.

Wyld (2010) proposed that an e-Government cloud must have the following eight characteristics:

- "Universal Connectivity — users must have near-ubiquitous access to the internet
- Open Access — users must have fair, non-discriminatory access to the internet
- Reliability — the cloud must function at levels equal to or better than current standalone systems
- Interoperability and User Choice — users must be able to move among cloud platforms
- Security — users' data must be safe

- Privacy — users' rights to their data must be clearly defined and protected
- Economic value — the cloud must deliver tangible savings and benefits
- Sustainability — the cloud must raise energy efficiency and reduce ecological impact".

2.3 Benefits of Cloud Computing for e-Government

There are several benefits to adopting cloud computing in e-Government. The main benefits can be categorized as follows:

- Availability and Accessibility

  One of the primary aims of e-Government is to provide readily available real time services to citizens. Cloud computing allows for access to services at any time and from any location, requiring only access to a PC and the Internet (Vijaykumar, 2011).
- Cost Effectiveness

  Utilizing a private cloud for e-Government reduces costs significantly by alleviating the need to purchase, install and update equipment and software. In addition, Zhang et al. (2010) estimated that around 53% of the cost of a datacentre relates to electricity and cooling in areas where these energy sources are costly, whereas cloud databases can be located in areas where the cost of energy is lower.
- Efficiency

  Providing public services efficiently and effectively to citizens and businesses is one of the main benefits of e-Government. The task is facilitated through cloud computing which allows for innovative use of technologically and economically feasible solutions. Cloud architectures can benefit government to reduce duplicate efforts and increase effective utilization of resources (Bhisikar, 2011); (Chanchary & Islam, 2011); (West, 2010).
- Flexibility and Scalability

  Cloud computing is a flexible and scalable technology due to its dynamic nature (AlAjmi, 2011).
- Transparency and Reduced Corruption

  The benefits of cloud computing include increasing transparency and deducing administrative corruption (Almunawar, 2015).

2.4 Cloud Computing in the Saudi Public Sector

In their study on '*The Determinants of Cloud Computing Adoption in Saudi Arabia*' , Alhammadi et al. (2015) highlighted three predictors of cloud readiness in Saudi Arabia; organisation readiness, top management support and enterprise status. Currently up to 70 % of Saudi government organizations have yet to adopt any type of cloud service, and of those only 33.5% plan to adopt a cloud service within the next two years (Al-Ruithe et al., 2017). From this it is clear why the few studies related to cloud computing in the public sector in Saudi Arabia focus on adoption.

Alsanea (2015) used a mixed methods approach to determine the factors affecting the adoption of cloud computing in Saudi Arabia's government sector. Mreea et al.(2016) on the other hand developed a value model to aid government organizations make the decision whether to adopt a cloud solution or to continue with in-house capabilities. Alassafi et al. (2017), focused on identifying the critical security factors that affect government organisations' decision to adopt cloud computing. Other studies have concentrated on a specific type of government organisation. Aharthi et al. (2017) identified the critical success factors for higher education institutions to migrate to the cloud and Alharbi et al. (2017) use a balanced scorecard approach to explore the value of adopting cloud computing in healthcare organisations.

In Saudi Arabia cloud computing is still in the early stages and there is a need to conduct studies that explore its implementation in the country (Mreea et al., 2016) (Al-Ruithe et al., 2017). This study is designed to fill the void in the research by identifying the CSFs specific to private government cloud implementation in Saudi Arabia. Using CSF to prepare for cloud implementation will '*mean greater probability of cloud success, with the organization more likely to reduce IT costs, achieve IT economies of scale, and redirect resources toward key business activities and core competencies that yield long-term competitive advantage*' (Garrison et al., 2012).

In the following sections, relevant literature is reviewed to pinpoint the challenges to implementing both cloud computing in Saudi Arabia in government in general and in government IT projects specifically in order to identify the factors that need to be mitigated to insure the success of a private government cloud in Saudi Arabia .

2.5 Challenges to Implementing Cloud Computing in Government

There are many noted challenges and obstacles to using cloud computing in general and to its use in e-Government in particular. Researchers have also found that the implementation of such projects in developing countries is more difficult than in developed ones (Schuppan, 2009). Literature focusing on the challenges to implementing cloud computing in government are summarised in Table 2. The main challenges to implementing cloud computing in government are described in the following sections.

System Failure

One of the two major risks for cloud computing users is a breakdown in the availability of service (Armbrust, et al., 2010), (AlAjmi, 2011). The most common forms of Service breakdowns are network outages that interrupt user access to the cloud service (AlAjmi, 2011). Service failure can affect user's trust in cloud computing (Alshomrani & Qamar, 2013).

Privacy and Security

When e-Government is based on cloud computing the privacy and security of personal data and information is a concern (Alshomrani & Qamar, 2013) . Cloud computing security concerns the "*confidentiality, availability and integrity of data or information*" (Karunanithi & Kiruthika, 2011). Jansen & Grance (2011) propose that security and privacy issues for cloud users and providers are an "*exercise in risk management*" and require constant monitoring of the system. Iglesias et al. (2012) note that while debate over data protection, privacy and interception laws with public clouds has been plentiful, private clouds, which can

be monitored more directly and accurately, have escaped much attention. Alshomrani & Qamar (2013) also identify lack of control over data centres, and fear of unauthorised access and data leakage as challenges for implementing cloud computing in government.

Legislation

There are several issues related to legislation and policy that could arise for government agencies using clouds, both as cloud users and as cloud providers (Armbrust, et al., 2010); (Jaeger et al., 2009); (Jansen & Grance, 2011). Janssen & Joha (2011) and Orakwue (2010) note the need to clarify data ownership and for awareness of legislation that applies not only in the country where the service is provided but also in the country where the cloud database is located.

Weber (2011) noted that the ownership of legislation governing data storage on computer servers beyond national borders or jurisdiction is an issue with cloud adoption. Buller (2016) noted that Saudi Arabia had issues related to data ownership, and a lack of cloud regulations and national cloud strategies, in response to which, the Saudi Communication and Information Technology Commission (CITC) has proposed the development of cloud computing regulations in the country (CITC, 2016).

Other Factors

Uncoordinated adoption and lack of appropriate organizational and governance mechanisms in place could undercut the benefits of SaaS (Janssen & Joha, 2011). Hodgkinson (2012) noted that the greatest risk mitigation would be to not compromise on the quality of enterprise grade compliance requirements. In addition, coordination and cooperation difficulties are proposed as factors (UK Cabinet Office, 2011). As further noted by Hodgkinson (2012) government services must support diverse processes, demands and priorities. Wyld (2010) observes that the main issues in the adoption of cloud computing are human, such as the resistance of IT personnel to change and retraining staff.

Table 2 Challenges to Implementing CC in Government

Source	Factors	Description	Challenges
(Yeh et al., 2010)		Highlight several issues to utilizing cloud computing for e-government	Data safety and privacy, Reducing of system reliability, Increase of the difficulties in service management as well as the Imperfectness of relevant laws
(Wyld, 2010)	Universal Connectivity, Open access, Reliability, Interoperability and User Choice, Security, Privacy, Economic value, Sustainability	Presented eight important factors for enabling cloud computing in the public sector	
(Kurdi et al., 2011)		Identified challenges to migrating e-government to cloud computing	Leadership, Strategy and BPR, Policy issues
(Janssen & Joha, 2011)		Found risks for adopting cloud-based software as a service (SAAS) in the public sector from Interviewing 13 IT experts from a variety of public organizations	Continuity, Performance, Privacy, Ensuring the control of the IT-function, and the Influence on further innovation and development directions
(AlAjmi, 2011)		Investigated the risks to introducing cloud computing in government	Standards for interoperability, Security, Availability, Crafting and enforcing policies and laws
(Liang, 2012)		Highlighted risks to government clouds	Security and privacy, Reliability and sustainability, Unified standards and legal support

Source	Factors	Description	Challenges
(Alshomrani & Qamar, 2013)		Present the challenges in cloud computing which can directly affect e-government	Privacy, Lack of user control, System Failure, Security, On Demand Self Service, Data Leakage
(Kooshesh et al., 2013)		Highlight challenges to implementing e-government based on cloud computing	Security policies, Network infrastructure, Security considerations, Appropriate laws
(Diez & SIlva, 2013)		Found that security and legal challenges are the primary concerns, for government clouds especially in public organizations in the EU under the Data Protection Directive another issue is integration with current systems	Security, Laws, Integration

2.6 Challenges to IT Projects in Saudi Arabia

Several success factors to implemnting IT projects in Saudi Arabia have been noted. Alfaadel et al. (2012) followed a mixed-method approach where they surveyed 308 IT project managers and interviewed eight project managers that work in both the Saudi public and private sector to identify the causes for success and failure of IT projects in Saudi Arabia. They found that reasons for the failure of IT projects in Saudi Arabia were suitable organizational culture, proper project planning, clear vision and objectives, clear statement of requirements, and lack of top management support. AlMajed & Mayhew (2013) conducted semi-structured interviews with ten CIO's with at least five years' experience in IT management to explore IT project success factors from the CIO's perspective. They noted several contributing factors including top management support and commitment, strategic planning, project

management, process management, project team competency, IT infrastructure, change management, risk management, communication management, training and education, supplier management, stakeholder management, conflict of interest, knowledge management, rewards and recognition, top management stability and PMO. In a later study, Almajed & Mayhew (2014) surveyed 72 CIO's in Saudi public organizations to identify CSF's for IT project success in Saudi Arabia and compare the outcomes with findings in Malaysia. Top management support and project management were concluded to be the top contributing factors in Saudi Arabia.

Studies investigating the critical success factors for implementing ERP projects in Saudi Arabia were also considered as ERP projects are large scale IT project. ALdayel et al. (2011) Surveyed IT staff and end-users to identify CSF for implementing ERP in a Saudi higher education institution and found project management, ERP selection, and the training offered to the end users to be critical factors. While Al-Turki (2011), conducted a survey of 93 different types of Saudi organizations, public and private, to investigate success factors for ERP implementation in Saudi Arabia and identified leadership, change management and training as contributing factors. In another ERP study, Saleh, Abbad, & Al-Shehri (2013) Survey 74 employees from mostly government or joint government- private owned organizations to determine the factors critical to the success of ERP implementation in Saudi Arabia and conclude vendor support, consultant competence, business process re-engineering, top management support and user support to be critical success factors.

Other studies were conducted to investigate the success factors for implementing government IT projects in Saudi Arabia. Abouzahra (2011) based on a four year survey and study of 52 public healthcare IT projects investigated the causes of success and failure in Healthcare Information Systems projects in Saudi Arabia, and identified the main causes of failure being unclear scope, failure to identify and analyse risks associated with data integration, incompatibility with existing systems and data inconsistency , failure to identify stakeholders in order to clearly define their requirements, and communication. In an alternative study, (Al-Mudimigh et al., 2011) use a case study implementing a portal in two government organizations to identify CSF's and recognise good

communication, user acceptance, top management support, clear goals and objectives, and project monitoring and controlling as critical factors.

2.7 Summary of Literature Review

The application of e-Government in Saudi Arabia is hindered by the weakness of the current ICT infrastructure in government agencies. A solution to this weakness is the adoption of a private government cloud. In order to facilitate this adoption, First, Cloud computing and its benefits to e-Government are explored. Then, the challenges facing the adoption of cloud computing in Saudi government agencies must be identified and mitigated. These challenges arise from the nature of cloud computing itself, as well as the environment of Saudi government agencies. In the previous sections, a literature review was conducted to identify the success factors for implementing a government cloud in Saudi Arabia. In the following chapter, these factors are synthesised to construct the framework for the successful implementation of a private government cloud.

Chapter 3: Development of Framework for Successful Implementation of a Government Cloud in Saudi Arabia (FSIGC)

From the previous chapter, it is clear that there are several challenges that governments face in the adoption of cloud computing; many of these challenges are universal, but there are also challenges that are specific to a particular region. Song et al. (2013) state that in order to introduce cloud computing in an organization, changes must be implemented. To date there has not been any research into what changes need to be made in order to make the introduction of cloud computing in Saudi Arabian government agencies successful. In this chapter a framework for the successful implementation of a private government cloud in Saudi Arabia is proposed. Section 3.1 explains the process followed to develop the framework. While section 3.2 describes the framework. Finally, the chapter is summarised in section 3.3.

3.1 FSIGC Development Process

As this is an exploratory study and factors will later be confirmed through a quantitative study, a systematic review was conducted using online research databases. To be included, studies must have occurred in a government setting, report on implementing cloud computing or a large scale IT project, and be available in English. Thematic analysis was followed to synthesize barriers and enablers to implementation a private G-cloud with the purpose of identifying the success factors. The framework for the successful implementation of a private G-cloud in Saudi Arabia was constructed in three stages.

Stage one involved determining, from relevant literature, the success factors for the implementation of a private government cloud. The determination process involved the following steps:

- Identification and review of published papers concerned with the implementation or adoption of cloud computing for government use
- Extraction of the factors that may challenge or enable the implementation of cloud computing in government from the concerned papers

- Exclusion of the factors that are not relevant to the implementation of a private cloud owned and managed by government, e.g. Contracts and service level agreements
- Re-definition of challenges as success factors
- Categorization and filtering of the relevant factors based on their meaning and scope for example identifying factors that have different names but have the same meaning of factors that are actually a component of another factor.

Stage one resulted in the identification of five success factors. These are security and privacy; reliability; policy and legislation; cooperation and coordination; and staff capability. However, success factors differ between developed and developing countries due to cultural differences (Alfaadel et al., 2012). This necessitated the identification of factors that are predominant due to the nature of the Saudi organisations. Thus far, there is a lack of literature on the implementation of cloud computing in Saudi Arabia. Consequently, literature related to the CSF for large scale IT projects were explored in the following stage.

Stage two involved identifying, from the relevant literature, the success factors for implementing large scale IT projects in Saudi Arabia, as the implementation of a private cloud is considered a large scale IT project. The following steps were applied in this stage:

- Identification of published papers concerned with the implementation of large scale IT projects in Saudi Arabian public organizations
- Extraction of the factors that may challenge or enable the implementation of large scale IT projects in Saudi Arabia from the concerned papers
- Exclusion of the factors related to citizen's adoption of systems because the purpose of this study is to facilitate G2G interaction by implementing a private G-cloud
- Re-definition of challenges as success factors
- Categorization and filtering of the relevant factors based on their meaning and scope

Six factors were identified from stage two: leadership and management; business process re-engineering; project planning; clear statement of requirements; top management support; and consultant and team competence. In the final stage, the factors identified in the previous stages were synthesized.

In *stage three*, the factors identified in stages one and two were synthesized (see Figure 4) to form the framework for the successful implementation of a private G-cloud in Saudi Arabia. See Table 3. This stage involved the following steps:

- Combining the success factors from stages one and two
- Categorization and filtering of the relevant factors based on their meaning and scope
- Removal of repeated factors

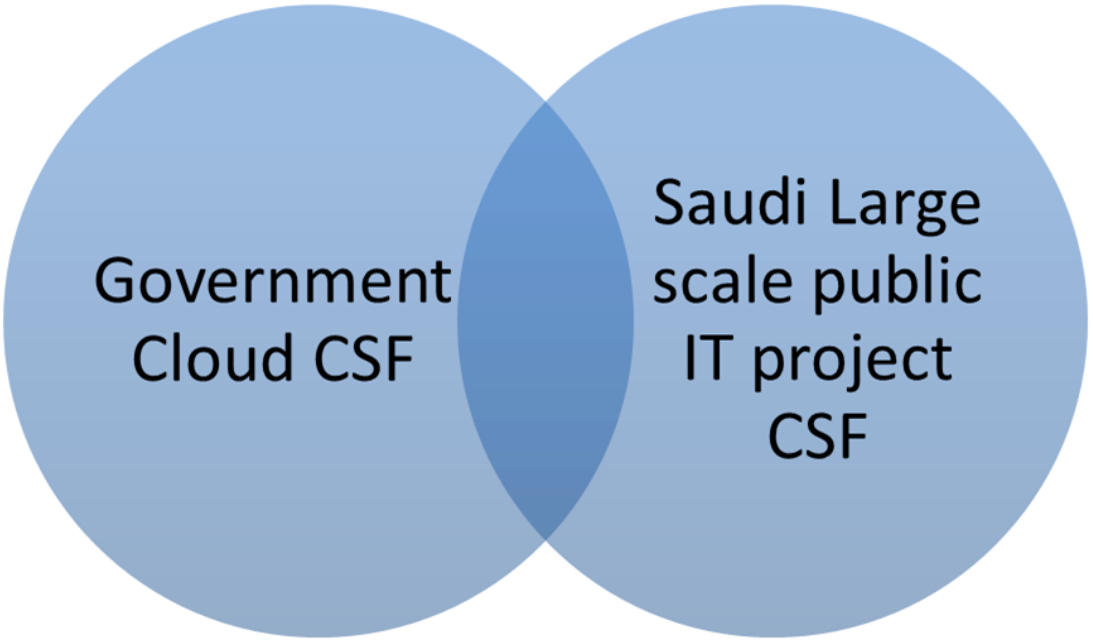

Figure 4 Research Area

Table 3 CSFs for Implementing a private G-cloud

Number	Challenge	Source
1	Security& privacy	(Yeh et al., 2010); (Wyld, 2010); (Janssen & Joha, 2011); (AlAjmi, 2011); (Liang, 2012); (Alshomrani & Qamar, 2013); (Kooshesh et al., 2013); (Diez & SIlva, 2013)
2	Reliability	(Yeh et al., 2010); (AlAjmi, 2011); (Wyld, 2010); (Janssen & Joha, 2011); (Liang, 2012); (Alshomrani & Qamar, 2013); (Kooshesh et al., 2013)
3	Cooperation and Coordination	(Wyld, 2010); (AlAjmi, 2011); (Diez & SIlva, 2013); (Abouzahra, 2011)
4	Policy and Legislation	(Yeh et al., 2010) (Kurdi et al., 2011); (Janssen & Joha, 2011); (AlAjmi, 2011); (Liang, 2012); (Kooshesh et al., 2013); (Diez & SIlva, 2013)
5	Leadership	(Kurdi et al., 2011); (Garrison et al., 2012); (ALdayel et al, 2011); (Al-Turki, 2011); (Almajed & Mayhew, 2014)
6	Business Process Re-Engineering	(Kurdi et al, 2011); (Saleh et al., 2013)
7	Project planning	(Abouzahra, 2011); (Al-Mudimigh et al., 2011); (Alfaadel et al., 2012); (AlMajed & Mayhew, 2013)
8	Clear requirements	(Abouzahra, 2011); (Al-Mudimigh et al., 2011); (Alfaadel et al., 2012)
9	Top management support	(Al-Mudimigh et al., 2011); (Alfaadel et al., 2012); (AlMajed & Mayhew, 2013); (Saleh et al., 2013), (Almajed & Mayhew, 2014)
10	Consultant competence	(Garrison et al., 2012); (Saleh et al., 2013)

3.2 Proposed FSIGC

The framework is comprised of ten components (Figure 5). These components cover technical, organizational and management aspects and are described in the following sections.

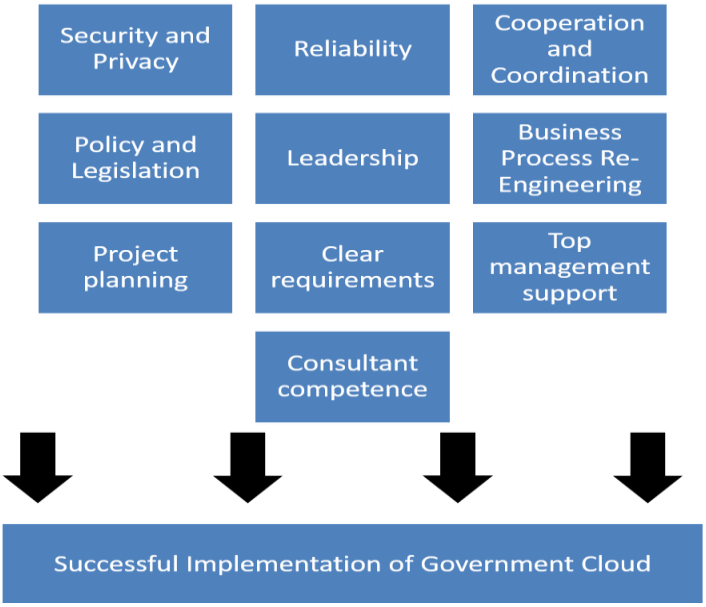

Figure 5 Proposed FSIGC

Security and Privacy

The sensitive nature of government data requires the adoption of strict security mechanisms and standards. Especially for authentication and identification. The implementation of a private cloud aids in overcoming some security issues.

Reliability

The IEEE defines Reliability as 'the ability of a system or component to perform its required functions under stated conditions for a specified period of time'. Government systems must be reliable and continuously available. Cloud solutions are dependent on the network. Therefore reliable standards and back up plans must be implemented.

Cooperation and Coordination

For the implementation of a private G-cloud, both technical coordination and organizational cooperation are required to insure interoperability.

Policy and Legislation

Cloud computing is a relatively new technology. It will require the implementation of governmental policies and legislations to insure the safety of stakeholders.

Leadership

Proper leadership is needed through all the stages of large scale projects such as the implementation of a private G-cloud. Leadership is required to explain, insure buy in and test the success of the project.

Business Process Re-Engineering (BPR)

To benefit completely from a private G-cloud, Business Process Re-Engineering is necessary. Government agencies will need to change how they perform their tasks.

Project planning

Planning is always important in government funded projects. However, it is vital in a project that requires co-operation and collaboration and the unification of standards, policies and processes such as the implementation of a private G-cloud.

Clear requirements

The first step in the implementation of a private G-cloud is collecting the requirements from various agencies each of which may have diverse needs. To ensure success, these requirements must be stated and communicated clearly to the team.

Top management support

For the success of any project, especially a large and complicated project such as implementation of a private G-cloud, top management support is essential. This support will ensure that the necessary resources and funds are provided.

Consultant competence

To insure the successful implementation of a private G-cloud in Saudi Arabia, the IT consultants and staff need to have the proper training and skills.

3.3 Chapter Summary

This chapter describes the process followed in the development of the FSIGC, after which the ten factors that form the FSIGC are defined . The success factors identified include: Security and Privacy, Reliability, Cooperation and Coordination, Policy and Legislation, Leadership, BPR, Project planning, Clear statement of requirements, Top management support, Consultant and Team competence. In the following chapter, the FSIGC is evaluated.

Chapter 4: Research Methodology

In this chapter, the FSIGC developed in Chapter 3: is evaluated. The chapter commences with an overview of the different research methods in 4.1. It them moves on in 4.2 to describing the methods applied in the current research to evaluate the FSIGC. The results are presented in 4.3 . Finally, the chapter is summarised in 4.4.

4.1 Research Methods

The techniques used to collect and analyse data are called methods. The two main methods used in information systems research are qualitative and quantitative, with a small portion of studies focusing on mixed methods (Recker, 2013). These three methods are discussed in detail in the following sections.

4.1.1 Qualitative Methods

Qualitative research methods involve collecting, analysing and interpreting data that cannot usually be presented in the form of numbers. They provide in depth understanding of a problem or situation. Hence, they are useful for exploratory research where a phenomenon is not well researched or is still developing (Recker, 2013).

There are four main types of qualitative methods: observation, interviews, documents and audio-visual materials (Creswell, 2013). The most commonly used method is interviews. Interviews are described as "*a conversation with a purpose*" (Preece et al., 2002).

Interviews are categorised as: open-ended or unstructured, structured and semi-structured, depending on the amount of control the interviewer holds over the interview (Preece, et al., 2002). The interviewer imposes control by determining a fixed set of questions prior to the interview. Another categorisation for

interviews is based on the number of participants. They can be one-to-one or a group interview. Each of these categories has its benefits (Preece, et al., 2002):

- Unstructured interviews: these usually produce rich data since the interviewees are given the opportunity to mention things that the interviewer may not have considered.
- Structured interviews: these are easier to analyse because the study is standardized. The same questions are given to each participant with a specific set of answers.
- Semi-structured interviews: these use both closed and open ended questions and share features with both structured and unstructured interviews.
- Focus groups or group interviews: these allow diverse or delicate issues to be raised and usually involve between three and ten people.

In qualitative research a large amount of data is produced and it is not always clear what parts of the data are relevant to the study. The most popular technique for analysing qualitative data is coding (Recker, 2013) (Creswell, 2013). Coding means assigning labels or meaning to chunks of data to categorise that data. Data is usually organised around the core ideas or themes found in the study. These codes may be determined prior to data collection or they may develop as the researcher is exposed to the data and broadens his perspective (Preece, et al., 2002). Tools such as Nvivo may be used to help researchers analyse and keep track of the data.

Due to the detailed and intense work required in qualitative research, it is necessary to limit sample size (Anderson, 2010); sample size is not decided based on mathematical calculations. The most important factor for sampling in quantitative studies is to recruit a diverse sample that is able to enlighten the research topic (King & Horrocks, 2010). This is called purposive sampling, where participants are chosen because they possess certain characteristics or expertise (Recker, 2013).

4.1.2 Quantitative Methods

Quantitative research involves collecting and analysing data that can be expressed in numbers. This research method is useful in confirmatory research where a previously developed theory needs to be confirmed (Recker, 2013).

One of the main methods for gathering quantitative data is questionnaires. A questionnaire consists of a set of questions for gathering participants' responses in a standardised manner. They can be used to collect demographic data and users' opinions. Their main benefit is that they can easily be circulated to a large number of respondents (Preece, et al., 2002).

The responses to questionnaire can be structured or unstructured. Structured responses are easier to capture and analysis. There are five formats for structured responses (Bhattacherjee, 2012):

- Dichotomous response: these allow for choosing from two possible responses
- Nominal response: these allow for choosing from more than two unordered responses
- Ordinal response: allow for choosing from more than two ordered responses
- Interval-level response: these allow for choosing from a 5-point or 7-point scale
- Continuous response: these usually include a blank space for the respondent to fill

Two different techniques are used for analysing quantitative data (Bhattacherjee, 2012): descriptive analysis where statistics are used to describe, combine and present the concepts of interest or show the relationships between these concepts, and inferential analysis where statistics are used to test a hypothesis. Software tools such as SPSS can aid in this analysis.

In quantitative studies it is important to recruit a sample that statistically represents the population in order to generalise the findings (King & Horrocks, 2010). This type of sampling is called random sampling where participants are chosen randomly from a wider population (Recker, 2013).

4.1.3 Mixed Methods

As a response to the criticisms faced by qualitative or quantitative methods a growing number of researchers are conducting mixed methods studies that explicitly combine both approaches (Recker, 2013). Moreover since qualitative methods are hard to generalise to a larger population (Recker, 2013), quantitative methods can be used to confirm the findings of qualitative data and generalise them. Also, collecting different types of data from diverse sources by different methods helps develop a clearer picture of the problem being studied (Kaplan & Duchon, 1988).

There are five major justifications for using mixed methods (Johnson & Onwuegbuzie, 2004):

- Triangulation: meaning that the findings of the study will be confirmed by using different methods to study the same problem
- Complementary: meaning that the findings from one method will be used to elaborate and clarify the findings from the other method
- Initiation: means using different methods to attempt to discover contradiction that will lead to reshaping the research questions
- Development: means that the findings from one method will be used to inform the other method
- Expansion: meaning that different methods will be used to study different problems to expand the scope of the research

Triangulation refers to using two or more methods to investigate a problem. It may be used for three different purposes: to validate the findings of a study, to generalise the findings, and to get better understanding of an issue (Jupp, 2006). Jick (1979) suggests that the use of multiple methods has the potential to reveal "unique variance" which may have been overlooked when applying a single method.

Triangulation has four main forms (Jupp, 2006):

- Data triangulation: which involves collecting data from different sources or people at different times.

- Investigator triangulation: which involves the data being collected and analysed by different investigators or researchers to mitigate the subjective impacts of individual investigators.
- Theoretical triangulation: which involves approaching data from different theoretical perspectives.
- Methodological triangulation: which involves using different methods to collect and analyse the same data to compare the findings.

4.2 Methods Applied in Preliminary Research

This preliminary study applies a mixed method approach to explore the factors influencing the success of a private government cloud in Saudi Arabia. The mixed method approach was chosen to strengthen the results of the study by validating the findings through triangulation (Kaplan & Duchon, 1988). In the next section a description is given of how the triangulation was performed and of the individual methods applied.

4.2.1 Triangulation

In order to refine and confirm the factors influencing the success of a private government cloud in Saudi Arabia a methodological triangulation was performed. It involved combining and comparing data gathered from a detailed literature review, an expert review and a questionnaire survey. The triangulation is performed in three stages since each method should be applied independently (Jupp, 2006). See Figure 6. The results from each stage were then compared.

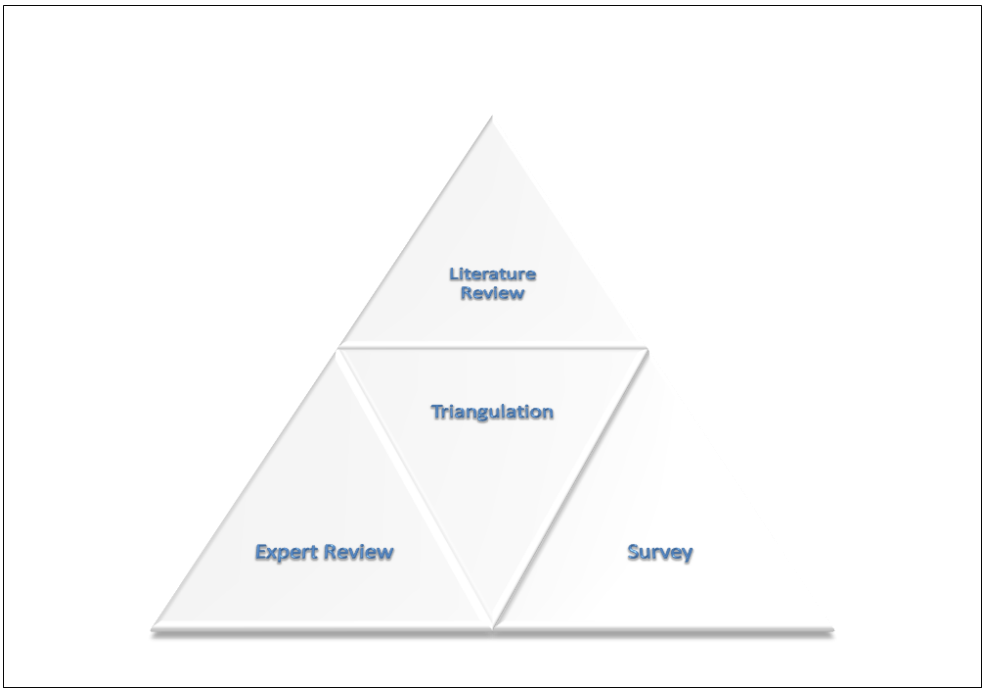

Figure 6 Triangulation Validation Method

First, data was collected from secondary research by reviewing related literature to build the framework proposed in Chapter 3: . Then, Interviews were conducted with experts to review the framework, in order to improve on (add, delete and modify components) the framework. Finally, an online survey was conducted to confirm the framework. See Figure 7.

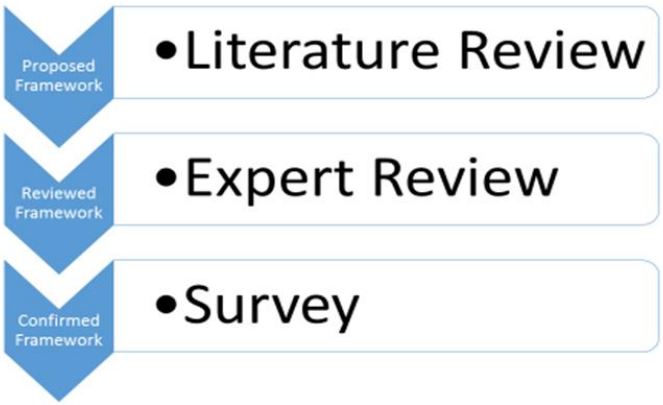

Figure 7 Research Methodology

4.2.2 Expert Review

Interviews were used to conduct an exploratory study since there is no basic framework for the successful implementation of a private government cloud in Saudi Arabia. The interview research method was chosen because it enables conducting in-depth discussions and explorations.

The initial framework proposed from the desk-based study was reviewed by interviewing experts working on IT projects in Saudi government agencies. Experts were chosen for interview at this exploratory stage since the findings from a sample of experts have more credibility than findings from a sample that includes non-experts (Bhattacherjee, 2012). The questions used for the interviews are shown in Appendix A.

4.2.2.1 Expert Review Sample Size

Qualitative studies usually depend on non-probability sampling where participants are chosen based on non-random criteria (Bhattacherjee, 2012). In expert sampling, participants are chosen based on their knowledge in the area being studied (Bhattacherjee, 2012). In this type of sampling, size depends on saturation (Guest, et al., 2006). Saturation is reached when no new knowledge can be gleaned. Guest, et al. (2006) suggests that saturation is usually reached by twelve interviews.

For the purpose of this review, twelve IT experts from different Saudi government agencies were interviewed. A person is considered an expert if they have at least five years' experience of working on IT projects within a Saudi government agency. All the experts approached agreed to take part in the interviews.

4.2.2.2 Ethics for Expert Review

Ethics approval (# 9509) was received to conduct these interviews from the University of Southampton's Ethics Committee. Interviewees were asked to read the Participant Information Sheet (Appendix G) and sign the Consent Form (Appendix H) before participating in the interviews.

4.2.2.3 Expert Review Process

The expert review was based on conducting semi-structured interviews with twelve IT experts from Saudi government agencies. These experts were from different Saudi government and semi-government organizations in different locations around Saudi Arabia. The interviews were conducted face-to-face, over the phone and online based on the availability and location of the expert. In the online interviews, the experts were asked to answer the questions and approached again for clarification when necessary. The two main objectives of these interviews were:

- To review the factors identified from the desk-based study conducted previously in order to improve on (add, delete and modify components) the framework
- To identify additional factors that are unique to the culture of Saudi government agencies that have not been mentioned previously in the literature

The semi-structured interviews included both closed and open questions. The closed questions were concerned with getting the experts' opinions on the factors in the proposed framework. Experts were also allowed to comment on these proposed factors. The open questions had the objective of identifying further factors that had not been identified in the desk-based study and to aid the researcher in understanding the current state of cloud computing in Saudi government agencies. Table 4 provides an overview of the interview question.

The interview questions were pre-tested on two Saudi IT experts and two fellow researchers at the University of Southampton to improve the clarity of the questions. Based on this pre-test, it was decided that rather than showing respondents a diagram of the framework and asking their opinion, the respondents will be asked their opinion on each individual framework component and allowed to make further comments. The questions were also modified based on the tests. The interview questions are provided in Appendix A.

Table 4 Interview Questions

NUMBER	QUESTION
1	Please state whether you find the following factors important and provide a reason for your choice: Security and Privacy, Reliability, Leadership, Project Planning, Clear Statement of Requirements, Top Management Support, Policy and Legislation, Consultant Competency, Cooperation and Coordination, BPR
2	What other factors do you recommend to ensure the successful implementation of a private G-cloud?
3	Does your organization use/ have used in the past cloud computing? If No, go to Q9
4	What type of cloud? (Public, Private or Hybrid)
5	What do you use the cloud for?
6	Are you satisfied with the services provided by the cloud?
7	Why are you satisfied/ dissatisfied?
8	What challenges did you face when implementing your cloud service?
9	What is stopping you from using cloud computing?

4.2.3 Survey

Questionnaires were chosen to confirm the updated framework resulting from the expert reviews. This approach was chosen for its ability to confirm and quantify the findings from quantitative research (Recker, 2013). This approach is favourable because it is an established method for capturing unobservable data such as participants' opinions, can be used to capture data about a large population that cannot be observed directly, and allows respondents to respond at their own convenience (Bhattacherjee, 2012).

4.2.3.1 Survey Sample Size

In qualitative research, random sampling is employed which allows the findings of the study to be generalized to the population (Bhattacherjee, 2012). Calculating random sample sizes is usually estimated mathematically based on preselected parameters (Guest, et al., 2006).

Two types of errors are considered when calculating the minimum acceptable sample size (Banerjee, et al., 2009). Type1 or α errors which occur when rejecting a true null hypothesis and type2 or β errors occur when a false null hypothesis is not rejected. The likelihood of these error occurring can be reduced by increasing the sample size (Banerjee, et al., 2009). By convention, α is set to 0.05 for a 95% confidence and (1-β) is set to 0.9 for 10% of missing an association (Banerjee, et al., 2009). Another parameter considered is effect size which refers to the magnitude of the association between the predictor and outcome variables. Cohen (1988) defines three different effect sizes: small (d=0.2), medium (d-0.5) and large (d=0.8). In exploratory studies effect size is usually set at large (Cohen, 1988).

In this study G* Power software (Faul et al, 2009) was used to calculate the minimum sample size. The calculation was performed for a t-test to find the difference in mean from constant. See Figure 8. From this calculation it was determined that the minimum sample size is 15.

4.2.3.2 Ethics for Survey

Ethics approval (# 9509) was received to conduct this survey from the University of Southampton's Ethics Committee. The Participant Information Sheet was displayed on the welcome page of the online questionnaire and check the box at the end of the page to indicate their consent to take part in the survey.

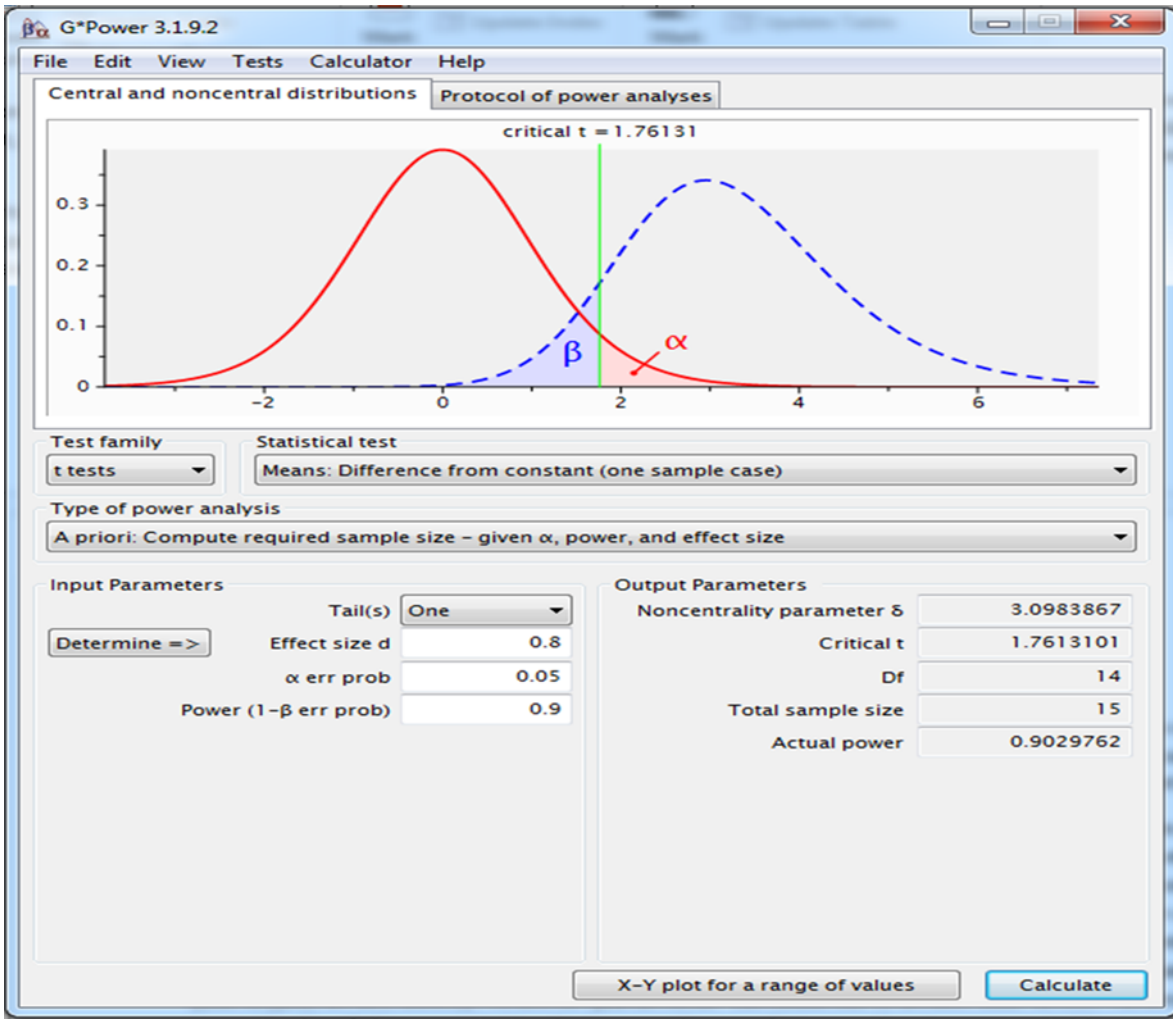

Figure 8 G Power Analysis

4.2.3.3 Survey Design

This survey was performed by administering an online questionnaire to confirm the factors in the updated framework resulting from the expert review. The questionnaire was designed based on findings from the interviews and is divided into two parts. The first part, asks three nominal questions about the respondents' organization type and experience to confirm their eligibility for this study.

The second part was constructed using a five point Likert-type scale (Bhattacherjee, 2012) with the following ratings: strongly agree = 1; agree = 2; neutral =3; disagree =4 and strongly disagree = 5. Scales are labeled verbally for respondents. Although numbers are easier to compute and remember, verbal

labels are easier for respondents to interpret (Krosnick & Fabrigar, 1997). Thus, improving reliability, validity and respondent satisfaction (Krosnick & Fabrigar, 1997).

The purpose of the questions in the second part is to confirm the proposed factors for the successful implementation of a private government cloud in Saudi Arabia. These factors are Security and Privacy, Reliability, Policy and Legislation, Standards, Knowledge Management, Cooperation and Coordination, Communication, Business Process Re-Engineering, Training, Top Management Support, Clear Statement of Requirements, Project Planning, Leadership, Consultant Competence, Business Continuity. Five of the factors are measured by more than one question. Consequently, twenty closed-ended questions reference the fifteen factors. The questions are shown in Table 5.

University of Southampton's iSurvey application was used to generate the online survey. Prior to administering the online questionnaire, it was pre-tested by five computer science researchers at the University of Southampton to ensure clarity of the questions. Their review was beneficial in reformulating some questions and improving the content of the survey.

It was decided to administer the questionnaire online as this method is convenient for respondents. Respondents were approached by email and social media and asked to complete the online questionnaire. Appendix B demonstrates the questionnaire.

Table 5 Survey Questions

No	Factor	To what extent do you agree that the following factors are important to the *successful* implementation of a private government cloud in Saudi Arabia?
1	Security and Privacy	The developed private cloud must be secure.
2		The developed private cloud must guarantee privacy.
3	Reliability	The developed private cloud must be reliable.
4	Policy and Legislation	Changes must be made in governmental policies to ensure the safety of all stakeholders in a private government cloud.
5	Standards	Standards governing information exchange between the different government entities must be improved.
6	Knowledge Management	Knowledge management must be undertaken throughout the lifecycle of the project.
7	Cooperation and Coordination	Cooperation between the various stakeholders is required.
8		Technical coordination is required to ensure interoperability.
9	Communication	Transparency throughout all stages of the implementation.
10		Giving regular updates and sharing information about the progress of the project.
11	Business Process Re-Engineering	Business Process Re-Engineering is necessary.
12	Training	Training must be provided for technical staff.
13		Training must be provided to end-users.
14	Top Management Support	Top management support is essential.
15	Clear Statement of Requirements	The requirements must be stated and communicated clearly to the development team.
16	Project Planning	Proper planning is vital.
17	Leadership	A project leader must be appointed to maintain all the information on the project and to coordinate between the different stakeholders.
18	Consultant Competency	IT consultants must have appropriate skills and knowledge.
19	Business Continuity	Business continuity must be considered.
20		Disaster recovery must be considered.

4.3 Analysis and Results of FSICC

As there are no previous studies on factors influencing the implementation of a private government cloud in Saudi Arabia, an exploratory study was performed. This study consisted of an expert review to evaluate and identify factors and a survey to confirm the identified factors. In this chapter, the results from both the expert review and the survey are presented and discussed.

4.3.1 Results of Expert Review

Twelve IT experts from different Saudi government agencies were interviewed. These experts had at least five years' experience in working on IT projects within Saudi government agencies. The purpose of this expert review was to review the possible factors identified from literature and to identify further factors. The reviews were constructed in the form of semi structured interviews that the researcher obtained permission to record. There were nine questions. The first question asked of the experts was to give their opinion on the importance of the proposed factors to the successful implementation of a private G-cloud. The remaining questions were used assess the state of cloud adoption within the sample experts and to identify additional factors.

4.3.1.1 Review of Proposed Factors

There was consensus among the respondents that all the proposed factors were important except for two anomalies. Expert B did not find ***Top Management Support*** an important factor. The expert stated that '*Usually this is not a factor to stop the project*'. Furthermore, expert F did not consider ***Reliability*** and ***Business Process Re-Engineering*** to be important since '*Privately ran cloud are more efficient than government operated setup*' and '*where IT services are hosted is not relevant to the actual business processes*'.

4.3.1.2 Cloud Adoption

Six of the experts in this study (50%) are working in organisations that already have adopted cloud computing. All of the experts are satisfied with their cloud implementation. Although, Expert B noted that "*All structure needs to be reviewed in terms of: security, business continuity and data protection*". The

private cloud deployment model is used predominately. While, two organisations are also using a hybrid cloud. Of the six non-adopters, four are planning to adopt some form of cloud. The remaining two state security concerns as their reason for not adopting a cloud model. Table 6 Highlight these results.

Table 6 Overview of Expert's Cloud Adoption

Expert	Adopter	Deployment Model	Satisfied	Reason for Non-adoption
A	Yes	Private	Yes	
B	Yes	Private, Hybrid	Yes	
C	No			Planning to adopt
D	Yes	Private, Hybrid	Yes	
E	Yes	Private	Yes	
F	Yes	Private	Yes	
G	No			Planning to adopt
H	No			Planning to adopt
I	Yes	Private	Yes	
J	No			Planning to adopt
K	No			Security
L	No			Security

4.3.1.3 Additional Factors

The experts' opinions were analysed and coded under two main headings Factors affecting the implementation of a private G-cloud and Challenges and Barriers to cloud implementation. The analysis highlighted five new factors Communication, Standards, Training, Knowledge Management, and Business Continuity.

Communication: Some of the experts stated having an effective and clear communication plan as a necessary factor for the successful implementation of

a private G-cloud. For example, **Expert G** highlighted communication as an important factor and stated that " *our IT projects suffer from the lack of communication*". **Expert C** also notes the importance of "*Communication Skills between staffs and communication speed between different locations*" as a factor. **Expert H** also notes the importance of "*Transparency (giving regular updates and sharing information about the progress of the project)".*

Standards: The availability of standards that govern cloud services is another factor emphasized by the experts. They felt that the lack of standards made it difficult to coordinate cloud projects. For example, **Expert F** states that "*Adapting and enforcing internationally accepted standards and frameworks to govern the provided cloud services is necessary*". **Expert G** also recommends "*Having specific indicators for measurement(standards)*". Similarly, **Expert H** mentions "*Setting Standards for information exchange between the different government entities*".

Training: Having the necessary training for the new system is an important factor for successful implementation. Several experts highlighted this factor. For instance, **Expert A** indorses "*Training for the IT team*" but, complains about "*Lack of local training facilities*". **Expert H** also recommends "*Training staff*". As does **Expert J** stating "*We need to train the staff on the new technology*".

Knowledge Management: Some experts emphasized that although knowledge management is an important factor for the successful implementation of a private G-cloud, they suffer from the lack of it in their organisations. Knowledge management is "*the process of creating, sharing, using and managing the knowledge and information of an organisation*" (Girard & Girard, 2015) . **Expert G** points out the need for "*Documentation (for transferring knowledge and continuing projects)*" and that " *When a consultant or employee leave, all their knowledge leaves with them*" and surprisingly " *We don't even inforce documentation for programmers!*". Similarly, **Expert H** recommends "*Knowledge transfer*" as a necessary factor.

Business Continuity: Another factor mentioned be experts is business continuity. A Business Continuity Plan is defined as "*the process of creating systems of prevention and recovery to deal with potential threats to a company"*

(Elliot, Swartz, & Herbane, 1999). For example, **Expert C** recommends having a "*Business Continuity Plan and Disaster Recovery Plan*" and states " *we learned the importance of this when we lost our data centre during a flood*". **Expert E** mentions that although they are satisfied with their current cloud implementation, "*different optimizations are becoming critical to be done. All structure needs to be reviewed in terms of: security, business continuity and data protection*".

Table 7 Recommended Factors

Factors	Themes
Security & Privacy	**Expert B** "*BCM and security are focused in data in cloud, rather than on systems in normal implementations*" and recommends these factors "*Data Knowledge and Awareness, Data Quality management, Data masking and Data protection*" **Expert D** faced issues with*" Security and Privacy*" **Expert F** found "*Security aspects" affecting implementation".*
Reliability	**Expert D** faced challenges with "*Reliability and Availability*"
Project Planning	**Expert A** states that it is important to "*Plan for the complete implementations of all the 3 Phases of the Private Cloud*" **Expert B** "*Push from management to complete projects on unrealistic schedules, resulting unsuccessful launching (or unsatisfying results)*" **Expert H** mentions "*Project management office*" as an important factor
Top Management Support	**Expert L** "*Sometimes we need information or work from the other departments and if the manager doesn't support us or make the request, we are ignored and the project is delayed*"
Policy & Legislation	**Expert F "***Legal aspects*" are challenging to the implementation and "*We believe the legislation and legal frameworks are the most pressing aspects to realize the anticipated growth in such services in KSA and in the region*"
Consultant Competency	**Expert A** "*Lack of local resources with Cloud Computing skills*" **Expert B** "*Cloud is tricky, and special skills become critical*"
Cooperation& Coordination	**Expert A** "*The most challenging task was the Data Center facilities preparation*" **Expert B** "*Different departments involved*" **Expert D & E** had issues with "*Interoperability and Portability*" **Expert F** stated "*Technical and Integration aspects*" as challenges to cloud implementation **Expert H** *"Compatibility with existing systems*" and" *Scheduling down time in order to work on fully utilized systems*"

Other factors mentioned were issues with vendors and Service Level Agreements, but, they were deemed to be unrelated to the implementation of a privately built and managed G-cloud. For example, **Expert A** complains that the cloud service provided by the vendor did not meet their expectations and notes "*We were expecting the product with the features with ease of use and self-service portal capabilities. But we are facing product limitations*". Similarly, **Expert G** also complains of vendors not fulfilling their contracts and recommends "*Knowledge and skills to conduct agreement with third parties (contractors) and awareness of SLA*"

The remainder of the factors deemed important by the experts are already mentioned in the framework in Chapter 3: The factors mentioned are Security and Privacy, Reliability, Project Planning, Top Management Support, Policy and Legislation, Consultant Competency, and Cooperation and Coordination. Table 7 gives an overview of the factors and the experts' comments.

4.3.2 Results of Survey

The questionnaire survey was conducted to confirm the factors identifies from the expert review. The questionnaire received responses from IT experts working in different Saudi government and semi-government organizations in diverse locations around Saudi Arabia. Thirty four participants completed the online survey but, four of those worked in the private sector with no government organisation experience and their responses were not relevant to this study. Thus, only thirty cases are considered in this study. Which is higher than the required minimum sample size of fifteen. The questionnaire was divided into two parts.

The first part, collected demographic data to determine the participants' eligibility for the study. Only respondents with at least two years' experience of working on IT projects in a Saudi government agency were considered. The type of organization the participant worked in was first deemed to be a factor for inclusion but, was later deemed inappropriate, since some respondents may be currently working in private organizations but, have previous experience of working in government organizations.

The purpose of second part was to collect participants opinions on the factors revealed after the expert review. This part consisted of twenty questions that covered fifteen factors. The responses to these questions were based on a five point Likert scale with 1 denoting 'Strongly Agree', 5 denoting 'Strongly Disagree' and 3 denoting 'Neutral'.

SPSS software was used to analyse the data. The hypothesis was tested for each factor using a one-sample t test with a test value of 3. The value 3 indicates Neutral on the five point Likert scale. The hypotheses for testing each factor are as follows:

H0: If the mean rating of the proposed factor < 3, then the factor affects the success of the implementation of a private G-cloud

H1: If the mean rating of the proposed factor ≥ 3, then the factor does not affect the success of the implementation of a private G-cloud

A Bonferroni correction was used in this study to reduce the possibility of having false positive results. Therefore, in this study an item (statement) is only statistically significant if the p-value < (α/n) 0.05/20 = 0.0025. This means that a null hypothesis is only rejected if the p-value is less than 0.0025. Table 8 shows the results of the analysis. From this table, it is clear that all the proposed factors were considered to have an effect on the success of a private G-cloud as they had an overall mean value of < 3. Furthermore, all the factors were found to be statistically significant as all the p-values are < 0.0025.

Table 8 Results of t test

#	Factor	Item	Mean	Sig. (2-tailed)
1	**Security and Privacy**	Security	1.03	<.001
		Privacy	1.13	<.001
2	**Reliability**	Reliability	1.20	<.001
3	**Policy and Legislation**	Policy and Legislation	1.67	<.001
4	**Standards**	Standards	1.30	<.001
5	**Knowledge Management**	Knowledge management	1.97	<.001
6	**Cooperation and Coordination**	Cooperation	1.43	<.001
		Coordination	1.40	<.001
7	**Communication**	Transparency	1.77	<.001
		Sharing information	1.67	<.001
8	**BPR**	Business Process Re-Engineering	1.80	<.001
9	**Training**	Training for technical staff	1.40	<.001
		Training for end-users	1.67	<.001
10	**Top Management Support**	Top management support	1.20	<.001
11	**Clear Requirements**	Clear requirements	1.30	<.001
12	**Project Planning**	Proper planning	1.30	<.001
13	**Leadership**	Project leader	1.30	<.001
14	**Consultant Competency**	Consultant competency	1.27	<.001

#	Factor	Item	Mean	Sig. (2-tailed)
15	**Business Continuity**	Business continuity	1.37	<.001
		Disaster recovery	1.20	<.001

The reliability of the survey results was determined using Cronbach's Alpha. Cronbach's alpha returned a value of 0.855. This value indicates that the reliability coefficient for the results is sufficient (Gliem & Gliem, 2003).

4.3.3 Discussion of Findings

The expert review confirmed the proposed factors and identified five additional factors. These factors were confirmed in the survey. In the following sections, the findings from both the expert review and survey are discussed.

4.3.3.1 Findings of Expert Review

From the expert review it was clear that over all the proposed factors were considered to be important by all of the experts except for Top Management Support, Reliability and Business Process Re-Engineering. For each of these factors one expert did not consider them to be important. As the majority of the results were found to be in agreement, the researcher did not find it necessary to remove these factors.

Five additional factors were determined by synthesising the expert suggestions. These factors are Communication, Standards for information exchange, Training for IT staff and end-users, Knowledge management, and Business continuity and disaster recovery plans. Other factors were suggested but were rejected, as they were found to be mentioned in the previously proposed factors or mot related to the purpose of this study.

4.3.3.2 Findings of Survey

From the survey, all the factors proposed from the desk based study and suggested in the expert review were deemed statistically significant. Security

and privacy received the most consensus. This shows that it is considered to be of high importance by experts. The confirmed framework for the successful of a private government cloud in Saudi Arabia is shown in Figure 9.

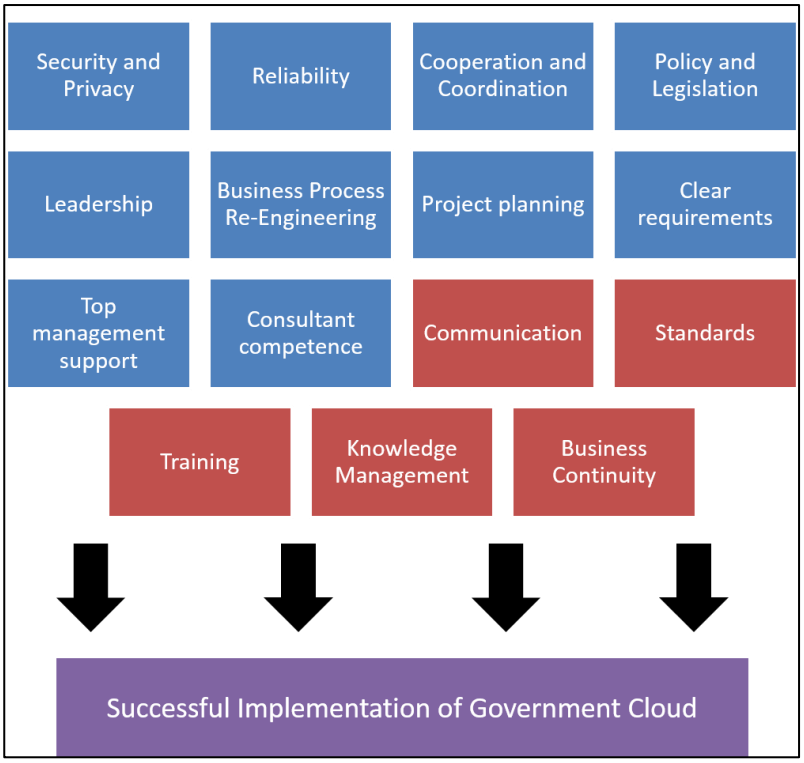

Figure 9 Confirmed Framework

4.4 Chapter Summary

There are no previous studies relating success factors for the implementation of a private government cloud in Saudi Arabia. Therefore an exploratory study was conducted to determine these factors. To review the factors proposed in a desk based study, an expert review involving twelve IT experts was performed. This review, confirmed the importance of the proposed factors an identified five further factors. These factors that comprise the FSIGC were confirmed via a questionnaire survey. In the following chapter, the FSIGC is applied in the development of the Government Cloud Readiness Measure.

Chapter 5: Development of Government Cloud Readiness Measure

In the previous chapter, a methodological triangulation was conducted to validate the factors that constitute the FSIGC. The results of the triangulation confirmed the FSIGC's fifteen factors.

Following the positive findings from the initial exploratory study and the validation of the factors, chapter 6 demonstrates the development and validation process for a novel measuring instrument. The Government Cloud Readiness Measure can be used to measure a government organization's readiness for implementing a private government cloud. The aim of this instrument is to aid Saudi government organisations in efficiently implementing private cloud solutions, in such that the degree to which an organization encompasses the confirmed factors is related to the degree to which they are ready to implement a private cloud, thus increasing the possibility of implementation success. The measure was developed through a stepwise approach using FSIGC as a reference guide during the development process highlighted in Section 5.1, after which items were generated for the Government Cloud Readiness Measure in Section 5.2. Finally, the chapter is summarised in Section 5.3.

5.1 Construction Process

To answer the second research question (*Are the proposed success factors being employed in Saudi government agencies ?*), an instrument is developed based on the factors identified and validated in the previous chapters. Instrument development is defined as, "the process of developing the data collection device in order to define and obtain relevant data for a given research question" (Dyba, 2000). While an instrument is defined aa device for measurement; in this study the instrument is in the form of a questionnaire. The purpose of this instrument is to measure a government organization's readiness for implementing a private cloud. After generating items for the instrument via a literature review , it was confirmed and validated through expert reviews and a survey. The process

followed for the development of the validated instrument is overviewed in Figure 10 and described in the following sections.

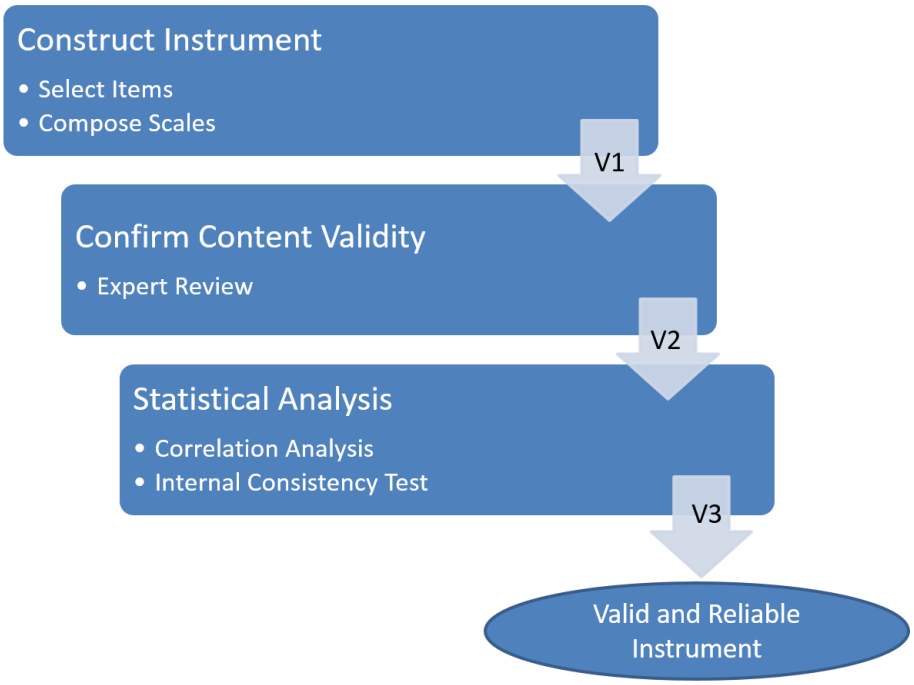

Figure 10 Overview of Instrument Development Process

5.2 Generating Items for Instrument

The instrument was developed based on the validated factors in the framework for successful implementation of a private government cloud shown in Chapter 4: . These factors represent the components of the instrument. Scales were proposed to measure each of these factors. De Vaus (2002) describes scales as '*a composite measure of a concept, a measure composed of information derived from several questions or indicators*'. Having multiple items to represent a component allow for a more true and reliable measurement (Dyba, 2000). The purpose of the scales in the government cloud readiness instrument is to measure the level of compliance in government organisations with the success factors suggested in FSIGC. Therefore, to reliably measure the level of compliance with cloud implementation success factors, multiple-item scales were developed such that more than one question is used to measure each factor. As combining multiple items gives a more accurate and reliable measure (Dyba, 2000). Scales were generated by reviewing literature and proposing items

to represent each of the factors. Each item is composed of a question and its associated 5-point scale. Table 9 presents a typical item.

Table 9 A Typical Item

		Always	Often	Sometimes	Rarely	Never
54	Communication plans are updated in my organisation.					

Several representative items were found for each factor to comprise the scales. An example of a scale in given in Table 10. A total of 85 items are proposed to represent the fifteen factors from the FSIGC. These items are presented in Table 11. The construction phase resulted in the development of the first version of the instrument shown in Appendix C.

Table 10 Scale for Communication Factor

Communication			Always	Often	Sometimes	Rarely	Never
	54	A formal communication plan is followed in my organisation.					
	55	Communication plans are updated in my organisation.					
	56	In the past communication has been effective in my organisation.					

Table 11 Factor Items

#	Factor	Potential Items	Total
1	**Security and Privacy**	IS security and privacy are given high priority in our organization A person/ department is appointed to manage security and privacy IS security and privacy is managed effectively in our organization. IS security and privacy training is provided for employees Our organization has specific IS security requirements. The requirements are standard-based The requirements are formalized in a policy document Our organization follows specific privacy laws/regulations. Our organization has limitations on international transfer of data	9 items
2	**Reliability**	IS reliability is given priority in our organization. A person/ department is appointed to manage IS reliability. I can count on the system being available when I need it Unreliable systems are changed/fixed System reliability is monitored Limits are set on acceptable system downtime	6 items
3	**Leadership**	Project managers are supported in our organization A project manager is designated for IS projects The project manager assigned is the best person for the job The project manager has a positive effect on project success The project team is happy to follow the PM Project managers are assigned based on specific requirements Training is provided for project managers	7 items

#	Factor	Potential Items	Total
4	**Project Planning**	Project planning is important in our organization A formal project plan is established before an IS project is started Project scopes are carefully defined A project team is designated for IS projects Realistic deadlines and budget are set Regular project status meetings are set Project plans are effective in our organization Training is provided on developing project plans	8 items
5	**Clear Requirements**	Requirements gathering is an important stage in IS projects Formal methods are used for gathering requirements IS project requirements are clear and complete Requirement gathering is done effectively in our organization	4 items
6	**Top Management Support**	Top management champion IS projects Top management provides projects with necessary resources Top management continuously monitor projects throughout their lifecycle Top management provide leadership for the project team	4 items
7	**Policy and Legislation**	There are existing local government legislation and policies that covers cloud computing These legislation and policies are sufficient These legislation and policies are effective Our organization has the competencies necessary to comply with these policies and legislations	4 items

#	Factor	Potential Items	Total
8	**Consultant Competency**	External IS consultants are given support We have formal processes for hiring/ (validating) external IS consultants External IS consultants are competent They have a positive effect on the success of IS projects External consultants are important to IS projects.	5 items
9	**Cooperation**	Cooperation is encouraged between all stakeholders in IS projects. Cooperation between IS project stakeholders is formalized. Cooperation is successful in our organization Cooperation between IS stakeholders is facilitated in our organization	4 items
	Coordination	Coordination of legacy systems with new IS is supported New systems are integrated with partner organization's systems Formal processes are followed for coordination Someone is assigned to manage coordination Coordination is successful	5 items
10	**BPR**	Organization is willing to adapt business processes to fit new systems A team is assigned to implement BPR Formal BPR strategies exist Enough time and resources are allocated to BPR BPR is effective in our organization Staff are trained on new business processes	6 items
11	**Communication**	Communication is a priority in or organization. We have a clear communication plan. Communication is effective.	3 items

#	Factor	Potential Items	Total
12	**Standards**	We have standards for exchanging information in our organization. The standards are managed by a person/group. We have a formal repository for information exchange Information exchange is successful Training is provided on information exchange standards	5 items
13	**Training**	Training for new systems is important in our organization When new systems are introduced in our organization, the training provided is adequate in length and detail Training improves the level of users' understanding Training gives users confidence in the new system Training is handled by knowledgeable and competent trainers	5 items
14	**Knowledge Management**	Our organization supports knowledge sharing. Our organization uses specific techniques and strategies for sharing knowledge Our organization uses technology for sharing knowledge (for e.g. Our organization provides training on knowledge sharing Our organization has strict laws on documentation	5 items
15	**Business Continuity**	Our organization have a Business Continuity and disaster recovery Plan Someone in our organization responsible for Business continuity management Our Business continuity plan is regularly reviewed and updated Business Continuity and disaster recovery procedures are documented Relevant staff trained to activate the BCDR plan	5 items
15 factors		**85 items**	

Responses

Each question in the instrument is accompanied by a subjective rating scale. A 5-point Likert scale was chosen because it produces higher reliability than the 3 or 7 point scales (Likert & Roslow, 1934). Responses are scores from 5 to 1, with 1 indicating "Strongly disagree", 2 indicating "Disagree", 3 indicating "Neutral", 4 indicating "Agree" and 5 indicating "Strongly Agree". "Strongly disagree" is the lowest possible score and implies almost no existence or compliance of the item in the organisation. On the opposite end, "Strongly agree" is the highest possible score and represents the existence or compliance of the item in the organisation. A rating of "Disagree", "Neutral" or "Agree" shows varying degrees of existence or compliance of the item in the organisation. The actual level of compliance with each factor is represented by the average of the item ratings for that factor. These sums are called 'Scale scores'. A government organization's chances of success with its cloud implementation program can be predicted via a vector of the scale scores for the fifteen factors. Table 12 explains the possible responses in detail.

Table 12 Response Rating Definition

Response	Definition
1 Strongly disagree	The item shows nonexistence of/compliance with corresponding factor
2 Disagree	The item shows minor existence of/compliance with corresponding factor
3 Neutral	The item shows acceptable existence of/compliance with corresponding factor
4 Agree	The item shows satisfactory existence of/compliance with corresponding factor
5 Strongly agree	The item shows ideal existence of/compliance with corresponding factor

5.3 Chapter Summary

This chapter followed the construction of a possible instrument for measuring government organisation's readiness for the implementation of a private cloud. The rating scale was constructed through the application of the components of the Frame work for the Successful Implementation of Cloud Computing presented in Chapter 3: . The proposed Government Cloud Readiness instrument will be validated and examined for reliability in the following chapter.

Chapter 6: Refining Private Government Cloud Readiness Measure

In the previous chapter, a government cloud readiness measure was proposed based on the FSIGC (see Chapter 3:). Since measurement instruments are expected to be valid and reliable (Dyba, 2000), the instrument' content validity was confirmed via an expert review in 6.1, after which a survey was conducted to confirm the instrument's reliability in Chapter 5: . The aim of the survry was to investigate the relationship between each item in a component and how they relate to the instrument as a whole. Finally, the chapter is summarised in 6.4.

6.1 Confirming Instrument

The first step in validating an instrument is ensuring content validity. According to Dyba (2000) "*content validity has to do with the degree to which the scale items represent the domain of the concept under study*". Content validity is a systematic process that involves examining the content to confirm that it represents the domain to be measured and is built into the process from the outset by choosing appropriate items (Davis, 1996); (Anastasi & Urbina, 1997). The content validation began in the item generation stage when a literature review was conducted to identify items for the instrument. Content validity is confirmed via an expert review explained in the following sections.

6.1.1 Content Validity

Ethics approval (#40067) was obtained from the University of Southampton's Ethics Committee to conduct the validation study. After which, the instrument was reviewed and confirmed by eleven IT project management and cloud computing experts with at least five years' experience. Of the panel of eleven experts, nine had a Ph.D. in computer science, four had IT management responsibility roles in Saudi government organisations and seven were researchers in universities. Interviews were chosen as a research method as they facilitate in-depth discussion and allow the participants to point out aspects not considered by the researcher. These experts were recruited based on their publications in the field of cloud computing and their roles in Saudi government

organisations. The interviews were conducted face-to-face to allow the participants to view the instrument and comment on each part. The aim of this expert review was to identify any additional items and to confirm that:

1. The selected items are adequate and relevant to the component they represent

2. The wording, responses, layout and length of the instrument are appropriate

3. The instrument is easy to read and understand

The interviews were semi-structured in that the experts were asked to comment on each item in the instrument and its relevance to the corresponding factor. After that, they were asked to suggest any additional items for the factor. Finally, they were shown a version of the instrument and asked to comment on its layout, responses and ease. See Appendix D for Expert Review questions.

Cronbach (1971) suggests a review process where experts in the area of the instrument review versions of it again and again until consensus is reached. Hence, interviews were conducted in three waves. At the end of each wave, the instrument was edited to reflect the suggested changes and a new version of the instrument was developed to be used in the next wave of interviews. Each wave concluded when no new data was identified. The results from each wave are highlighted in the following sections:

6.1.2 Results of Content Validity

Wave 1

In Wave 1 the experts were asked to review Verion1 of the instrument. Several changes were made to the original instrument based on the Experts' recommendations. Items were deleted and others were added such that from an initial pool of 85 items, the refined instrument now consists of 71 items (refined list of items is shown in Table 13). The changes included:

- Changes to the wording of the instrument such as including the phrase "in my organisation" to insure that responders answer about the organisation they work in

- Splitting security and privacy into two sections to improve their representation and clarity. Similarly, Cooperation and Coordination are split to improve precision.
- Changing the responses from measuring agreement to measuring frequency in the form “Never”, “Rarely”, “Sometimes”, “Often” and “Always”. For labels to be beneficial, they are required to have reasonably precise meanings for the respondents (Krosnick & Fabrigar, 1997). Hence, It was deemed necessary to make the change based on experts’ opinion felt it gave a more accurate meaning.
- Examples were added to clarify some of the questions
  Version two of the instrument is found in Appendix E.

Wave 2

In Wave 2 experts were shown Version 2 of the instrument. Only one item was added to the instrument after this review. The item “Top management in my organisation understands the benefits of migrating to the cloud” was added to represent ‘Top Management Support’. Increasing the number of items to 72. The third version of the instrument is displayed in Appendix F.

Wave 3

In the final wave the expert were shown version 2 for review. Responses were positive and no changes were made to the third version, shown in Appendix F, of the instrument. Thus, the instrument is refined and ready for statistical validation in the following section.

Table 13 Refined Item List

Factor	Items	Total
Security	Information security is given high priority in my organisation A person/ department is appointed to manage information security policies in my organisation Information security is managed effectively in my organisation Information security training is provided for employees in my organisation International Information security standards are implemented in my organisation(ex. ISO 27001 and ISO 27002) International Cloud security standards are implemented in my organisation (ex. ISO 27017 and Cobit Cloud) Information Security standards are formalised and followed in my organisation	7
Privacy	Privacy is given high priority in my organisation Privacy is managed effectively in my organisation Information privacy training is provided for employees in my organisation International privacy standards are implemented in my organisation (ex. ISO/IEC 27018)	4
Reliability	Information system reliability is given priority in my organisation I can count on information systems being continuously available in my organisation Unreliable information systems are immediately repaired or changed in my organisation Maximum acceptable downtime limits are set for each system in my organisation Precaution measures are put in place to avoid information system downtime in my organisation	5
Leadership	Top management supports information system project managers in my organisation Qualified project managers are assigned to information system projects in my organisation In the past, project managers contributed to the success of information system projects in my organisation	3

Factor	Items	Total
Project Planning	Information system project planning is a priority in my organisation A specific project team is assigned to information system in my organisation Project plans are effective for the success of information system projects in my organisation Project plans are approved by top management in my organisation Information system project plans are based on international standards in my organization (ex. PRINCE2/PMP)	5
Clear requirements	Requirements gathering is an important stage for information system projects in my organisation A formalised process is followed for gathering information system requirements in my organisation Information system project requirements are clear in my organisation Information system requirement gathering is done effectively in my organisation	4
Top management support	Top management support information system projects in my organisation Top management provides information system projects with necessary resources in my organisation Top management continuously monitor information system projects throughout their lifecycle in my organisation Top management rewards/ penalizes teams working on successful/ failed information system projects in my organisation	4
Policy and legislation	There are existing local government legislations and policies that cover cloud computing Existing local government legislation and policies are effective My organization has the competencies necessary to comply with local policies and legislations	3

Factor	Items	Total
Consultant competency	External information system consultants are given support in my organisation There is a formal process for hiring external information system consultants in my organisation Previous external information system consultants have been competent External information system consultants follow a formal consulting process in my organization External information system consultants are hired based on competency in our organization (i.e. not based on lowest cost)	5
Cooperation	Cooperation is encouraged between all information system stakeholders in my organisation Cooperation between information system project stakeholders is formalized in my organisation On past information system projects in our organisation, cooperation between stakeholders was successful	3
Coordination	Coordination of legacy systems with new information systems is supported in my organisation Coordination of partner organisation's systems with new information systems is supported in my organisation Personnel are dedicated to oversee coordination of information systems in my organisation In the past, coordination of information systems has been successful in my organisation	4
Business Process Re-engineering (BPR)	Information systems are adapted to fit new business processes in my organisation BPR strategies are formalised and followed in my organisation Systems are adapted successfully to fit new business processes in my organisation Training is provided for resources when new business processes are introduced in my organisation BPR is aligned with existing processes in my organization	5

Factor	Items	Total
Communication	A formal communication plan is followed in my organisation Communication plans are updated in my organization In the past communication was effective on information system projects in my organisation	3
Standards	Information exchange follows international standards in my organisation A formal repository for information exchange is available in my organisation The exchange of information is effective in my organisation	3
Training	Training for new information systems is given priority in my organisation Training improves the level of users' understanding of new information systems in my organisation Training gives users' confidence in using new information systems in my organisation Training sessions are taught by qualified professionals in my organisation Training materials are updated in my organization Help desks are available to provide post –training support in my organization	6
Knowledge Management	Formal techniques and strategies are used for sharing knowledge in my organisation Technology is utilised for sharing knowledge in my organisation Knowledge sharing is monitored in my organization	3
Business Continuity	A Business Continuity and Disaster Recovery plan exists in my organisation Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan in my organisation Business Continuity and Disaster Recovery plans are based on international standards in my organization(ex ISO 22301) Existing Business Continuity and Disaster Recovery plans are sufficient to insure business continuity in my organization	4
Total		71

6.2 Statistical Analysis

After confirming the content validity of the instrument, a survey study was conducted by distributing it to a sample of respondents and analysing the results. The aim of this study was to test:

1. The relationship between the items in a component
2. The relationship between items and their component
3. The relationship between components and the instrument

IT employees working in Saudi government organizations were invited to participate in an online questionnaire. Sample size was set at 150 as it is recommended to have at least ten respondents per component (Bartlett, Kotrlik, & Higgins, 2001) and between 100 and 200 respondents to ensure accurate item analysis (Spector, 1992). The participants were recruited from the database of oversees Saudi students, via the websites and social media accounts of Saudi government organizations, and by visiting the IT offices of willing government organizations.

337 people attempted the online survey but, only 156 completed it. Of those, 153 were deemed usable for the study. The responses were used to confirm the reliability of the instrument. The analysis of the responses was performed using SPSS software. Cronbach's alpha and Pearson's r are used to validate the reliability of the instrument. Both tests were chosen for their ability to demonstrate the strength of the association between the items in a component, between items and the component they represent, and between the components and the instrument. Items are considered for deletion where item-item and item-scale correlations are low and the value of alpha raised if deleted. At the conclusion of this phase, a validated instrument is developed.

6.2.1 Correlation Analysis

Correlation is used to investigate the relationship between two variables. The correlation coefficient, Pearson's r, denotes the strength of the relationship between variables. It ranges between 1 and -1, With 1 representing a perfect positive relationship and -1 representing a perfect negative relationship. While 0 represents no relationship at all. The closer the correlation coefficient is to 1 or -1 indicates the strength of the relationship while sign (+ or -) indicates the direction of the relationship. Cohen (1988) recommends assessing the strength of a relationship using the following guidelines:

- $0.1 <| r |< 0.29$ weak correlation
- $0.3 <| r |< 0.49$ moderate correlation
- $0.5 <| r |< 1.0$ strong correlation

Using a correlation matrix can show the strength of the relationship between variables. It also aids in determining if there is no relationship between variables. In the following sections, describe the correlation matrices for all the factors in the instrument as well as each factor on its own.

6.2.1.1 Correlation among Factors

Table 14 shows the correlation matrix for all the factors in the instrument. The results show a significant correlation for all factors in the instrument. Each factor is significantly correlated to the other factors in such that $0.5 <| r |< 1.0$ and $p < 0.01$. Although, Security is highly correlated to Privacy with $r(153)= .918$ and Cooperation is highly Coordination with $r(153)= .903$, this is not cause for concern. Such a high value may require investigation into whether these items are redundant but, they are actually one factor split into two components for the purpose of clarity. This was done based on the recommendations of experts during the content validation study. In the following sections the item correlation for each individual factor is explored.

Table 14 Correlation Matrix for Cloud Readiness Factors

		Sec	Prv	Rel	Led	PP	ClReq	TM	PL	CC	Coop	Coor	BPR	Com	Std	Trn	KM	BC
Sec	Pearson Correlation	1	.918**	.820**	.789**	.823**	.733**	.754**	.678**	.816**	.786**	.800**	.823**	.695**	.868**	.765**	.795**	.828**
Prv	Pearson Correlation		1	.798**	.776**	.798**	.746**	.732**	.750**	.779**	.792**	.805**	.842**	.775**	.866**	.756**	.804**	.789**
Rel	Pearson Correlation			1	.762**	.773**	.653**	.568**	.655**	.761**	.828**	.854**	.786**	.604**	.792**	.625**	.772**	.739**
Led	Pearson Correlation				1	.862**	.729**	.770**	.680**	.830**	.817**	.810**	.814**	.690**	.798**	.756**	.739**	.789**
PP	Pearson Correlation					1	.803**	.835**	.694**	.856**	.787**	.817**	.811**	.754**	.818**	.767**	.704**	.781**
ClReq	Pearson Correlation						1	.808**	.680**	.720**	.684**	.667**	.734**	.733**	.729**	.685**	.619**	.680**
TM	Pearson Correlation							1	.683**	.802**	.681**	.660**	.738**	.750**	.720**	.799**	.621**	.710**
PL	Pearson Correlation								1	.685**	.670**	.615**	.690**	.736**	.746**	.622**	.730**	.642**
CC	Pearson Correlation									1	.797**	.789**	.833**	.759**	.836**	.801**	.757**	.812**
Coop	Pearson Correlation										1	.903**	.873**	.660**	.863**	.749**	.836**	.807**
Coor	Pearson Correlation											1	.881**	.628**	.867**	.764**	.796**	.831**
BPR	Pearson Correlation												1	.743**	.894**	.837**	.853**	.848**
Com	Pearson Correlation													1	.753**	.724**	.654**	.633**
Std	Pearson Correlation															.793**	.861**	.884**
Trn	Pearson Correlation															1	.735**	.772**
KM	Pearson Correlation																1	.789**
BC	Pearson Correlation																	1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.2 Correlations for Security (Sec)

Table 15 shows the results from the Security factor. The second item 'A person is appointed to manage security' is significantly correlated to 'security is managed effectively' with $r(153)= .827$, 'security training is provided' with $r(153)= .580$, 'security standards are implemented' with $r(153)= .729$, 'Cloud security standards are implemented' with $r(153)= .664$, and 'Security standards are formalised and followed' with $r(153)= .746$, (all $p < 0.01$). Although, the item 'Information security is given priority' is showing weak correlations with all other items in the factor, it not removed until considering its reliability score.

Table 15 Correlations for Security Factor

		Sec1	Sec2	Sec3	Sec4	Sec5	Sec6	Sec7
Sec1	Information security is given high priority	1	.207*	.216**	.219**	.109	.088	.173*
Sec2	A person is appointed to manage information security policies		1	.827**	.580**	.729**	.664**	.746**
Sec3	Information security is managed effectively			1	.634**	.766**	.724**	.819**
Sec4	Information security training is provided				1	.622**	.591**	.635**
Sec5	International Information security standards are implemented					1	.823**	.788**
Sec6	International Cloud security standards are implemented						1	.747**
Sec7	Information Security standards are formalised and followed							1

Correlation is significant at the 0.05 level (2-tailed).*

Correlation is significant at the 0.01 level (2-tailed).**

6.2.1.3 Correlations for Privacy (Prv)

The correlation results for the Privacy factor are presented in Table 16. The second item 'Privacy is managed effectively' is significantly correlated to 'Privacy is given high priority' with $r(153) = .340$, 'Privacy training is provided' with $r(153) = .681$, and 'International privacy standards are implemented' with $r(153) = .809$, (all $p < 0.01$).

Table 16 Correlations for Privacy Factor

		Prv1	Prv2	Prv3	Prv4
Prv1	Privacy is given high priority	1	.340**	.273**	.118
Prv2	Privacy is managed effectively		1	.681**	.809**
Prv3	Privacy training is provided			1	.672**
Prv4	International privacy standards are implemented				1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.4 Correlations for Reliability (Rel)

The results from Table 17 show that 'Information systems are continuously available' is significantly correlated with 'Unreliable information systems are changed' with $r(153)= .904$, 'Downtime limits are set' with $r(153)= .756$, and 'Precaution measures are put in place' with $r(153)= .792$, (all $p < 0.01$). Although, the item 'Reliability is given priority' is showing weak correlations with all other items in the factor, it not removed until considering its reliability score.

Table 17 Correlations for Reliability Factor

		Rel1	Rel2	Rel3	Rel4	Rel5
Rel1	Reliability is given priority	1	.234**	.205*	.161*	.198*
Rel2	Information systems are continuously available		1	.904**	.756**	.792**
Rel3	Unreliable information systems are changed			1	.743**	.813**
Rel4	Downtime limits are set				1	.856**
Rel5	Precaution measures are put in place					1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

6.2.1.5 Correlations for Leadership (Led)

From Table 18 it is clear that 'Qualified project managers are assigned' is significantly correlated to 'Management supports information system project managers' with $r(153)= .693$, and 'Project managers contributed to the success of information system projects' with $r(153)= .828$, (all $p < 0.01$).

Table 18 Correlations for Leadership Factor

		Led1	Led2	Led3
Led1	Management supports information system project managers	1	.693**	.684**
Led2	Qualified project managers are assigned		1	.828**
Led3	Project managers contributed to the success of information system projects			1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.6 Correlations for Project Planning (PP)

The results from Table 19 show that 'Project plans are effective' is significantly correlated with 'Project planning is a priority', $r(153)= .424$, 'A specific project team is assigned', $r(153)= .754$, 'Project plans are approved by top management', $r(153)= .722$, and 'Project plans are based on international standards', $r(153)= .792$, (all $p < 0.01$).

Table 19 Correlations for Project Planning Factor

	PP1	PP2	PP3	PP4	PP5
PP1 Project planning is a priority	1	.248**	.424**	.345**	.435**
PP2 A specific project team is assigned		1	.754**	.719**	.740**
PP3 Project plans are effective			1	.722**	.792**
PP4 Project plans are approved by top management				1	.705**
PP5 Project plans are based on international standards					1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.7 Correlations for Clear Requirements (ClReq)

The correlation results in Table 20 display that 'Requirements gathering is an important stage' is significantly correlated to 'A formalised process is followed', $r(153)= .438$, 'Project requirements are clear', $r(153)= .389$, and 'Requirement gathering is done effectively', $r(153)= .470$, (all $p < 0.01$).

Table 20 Correlations for Clear Requirements Factor

	ClReq1	ClReq2	ClReq3	ClReq4
ClReq1 Requirements gathering is an important stage	1	.438**	.389**	.470**
ClReq2 A formalised process is followed		1	.667**	.664**
ClReq3 Project requirements are clear			1	.807**
ClReq4 Requirement gathering is done effectively				1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.8 Correlations for Top Management Support (TM)

The results in Table 21 show that 'Support information system projects' is significantly correlated to 'Provide information system projects with necessary

resources', $r(153) = .708$, 'Continuously monitors information system projects', $r(153) = .638$, 'Rewards/ penalties', $r(153) = .523$, and 'Understands the benefits of migrating to the cloud', $r(153) = .526$, (all $p < 0.01$).

Table 21 Correlations for Top Management Support Factor

		TM1	TM2	TM3	TM4	TM5
TM1	Support information system projects	1	.708**	.638**	.523**	.526**
TM2	Provide information system projects with necessary resources		1	.766**	.643**	.750**
TM3	Continuously monitors information system projects			1	.646**	.748**
TM4	Rewards/ penalties				1	.626**
TM5	Understands the benefits of migrating to the cloud					1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.9 Correlations for Policy and legislation (PL)

From Table 22 it is clear that the item 'Local government legislation and policies are effective' is significantly correlated to 'Existing local government legislations and policies cover cloud computing', $r(153) = .322$ and 'My organization has the competencies necessary to comply', $r(153) = .746$, (both $p < 0.01$).

Table 22 Correlations for Policy & Legislation Factor

		PL1	PL2	PL3
PL1	Existing local government legislations and policies cover cloud computing	1	.322**	.190*
PL2	Local government legislation and policies are effective		1	.746**
PL3	My organization has the competencies necessary to comply			1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

6.2.1.10 Correlations for Consultant Competency (CC)

The results in Table 23 show that the item 'Consultants are given support' is significantly correlated to 'There is a formal process for hiring consultants', $r(153) = .675$, 'Consultants have been competent', $r(153) = .619$, 'Consultants

follow a formal consulting process', $r(153) = .658$, 'Consultants are hired based on competency', $r(153) = .630$, (all $p < 0.01$).

Table 23 Correlations for Consultant Competency Factor

	CC1	CC2	CC3	CC4	CC5
CC1 Consultants are given support	1	.675**	.619**	.658**	.630**
CC2 There is a formal process for hiring consultants		1	.738**	.805**	.729**
CC3 Consultants have been competent			1	.701**	.690**
CC4 Consultants follow a formal consulting process				1	.829**
CC5 Consultants are hired based on competency					1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.11 Correlations for Cooperation (Coop)

The correlation results for the Cooperation Factor are displayed in Table 24. The results show that the item 'Cooperation is encouraged' is significantly correlated to 'Cooperation is formalized', $r(153) = .798$ and 'Cooperation has been successful', $r(153) = .835$, (both $p < 0.01$).

Table 24 Correlations for Cooperation Factor

	Coop1	Coop2	Coop3
Coop1 Cooperation is encouraged	1	.798**	.835**
Coop2 Cooperation is formalized		1	.803**
Coop3 Cooperation has been successful			1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.12 Correlations for Coordination (Coor)

The results in Table 25 show that the item 'Coordination of information systems is successful' is significantly correlated with 'Coordination of legacy systems with new information systems is supported', $r(153) = .819$, 'Coordination with partner organisation's systems is supported', $r(153) = .871$, and 'Personnel are dedicated to oversee coordination', $r(153) = .835$, (all $p < 0.01$).

Table 25 Correlations for Coordination Factor

		Coor1	Coor2	Coor3	Coor4
Coor1	Coordination of legacy systems with new information systems is supported	1	.891**	.747**	.819**
Coor2	Coordination with partner organisation's systems is supported		1	.770**	.871**
Coor3	Personnel are dedicated to oversee coordination			1	.835**
Coor4	Coordination of information systems is successful				1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.13 Correlations for Business Process Re-engineering (BPR)

From Table 26 it is clear that 'Information systems are adapted to fit new business processes' is significantly correlated with 'BPR strategies are formalised and followed', $r(153) = .777$, 'Systems are adapted successfully to fit new business processes', $r(153) = .831$, 'Training is provided when new business processes are introduced', $r(153) = .704$, 'BPR is aligned with existing processes', $r(153) = .765$, (all $p < 0.01$).

Table 26 Correlations for BPR Factor

		BPR1	BPR2	BPR3	BPR4	BPR5
BPR1	Information systems are adapted to fit new business processes	1	.777**	.831**	.704**	.765**
BPR2	BPR strategies are formalised and followed		1	.869**	.784**	.848**
BPR3	Systems are adapted successfully to fit new business processes			1	.835**	.864**
BPR4	Training is provided when new business processes are introduced				1	.809**
BPR5	BPR is aligned with existing processes					1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.14 Correlations for Communication (Com)

The results in Table 27, highlight that the item 'Communication has been effective' is significantly correlated to 'A formal communication plan is followed',

$r(153) = .549$ and 'Communication plans are updated', $r(153) = .807$, (both $p < 0.01$).

Table 27 Correlations for Communication Factor

		Com1	Com2	Com3
Com1	A formal communication plan is followed	1	.469**	.549**
Com2	Communication plans are updated		1	.807**
Com3	Communication has been effective			1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.15 Correlations for Standards (Std)

The results presented in Table 28 show that the item 'The exchange of information is effective' is significantly correlated with 'Information exchange follows international standards', $r(153) = .864$ and 'A formal repository for information exchange is available', $r(153) = .808$, (both $p < 0.01$).

Table 28 Correlations for Standards Factor

		Std1	Std2	Std3
Std1	Information exchange follows international standards	1	.846**	.864**
Std2	A formal repository for information exchange is available		1	.808**
Std3	The exchange of information is effective			1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.16 Correlations for Training (Trn)

The results from Table 29 highlight that the item 'Training for new information systems is given priority' is significantly correlated to 'Training improves the level of users' understanding of new information systems', $r(153) = .568$, 'Training gives users' confidence in using new information systems', $r(153) = .552$, 'Training sessions are taught by qualified professionals', $r(153) = .718$, 'Training materials are updated', $r(153) = .717$, and 'Help desks are available to provide post –training support', $r(153) = .702$, (all $p < 0.01$).

Table 29 Correlations for Training Factor

		Trn1	Trn2	Trn3	Trn4	Trn5	Trn6
Trn1	Training for new information systems is given priority	1	.568**	.552**	.718**	.717**	.702**
Trn2	Training improves the level of users' understanding of new information systems		1	.825**	.626**	.661**	.554**
Trn3	Training gives users' confidence in using new information systems			1	.663**	.636**	.586**
Trn4	Training sessions are taught by qualified professionals				1	.843**	.724**
Trn5	Training materials are updated					1	.721**
Trn6	Help desks are available to provide post –training support						1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.17 Correlations for Knowledge Management(KM)

Results from Table 30 show that the item 'Formal techniques and strategies are used for sharing knowledge' is significantly correlated to 'Technology is utilised for sharing knowledge', $r(153)= .836$ and 'Knowledge sharing is monitored', $r(153)= .830$, (both $p < 0.01$).

Table 30 Correlations for Knowledge Management Factor

		KM1	KM2	KM3
KM1	Formal techniques and strategies are used for sharing knowledge	1	.836**	.830**
KM2	Technology is utilised for sharing knowledge		1	.805**
KM3	Knowledge sharing is monitored			1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.1.18 Correlations for Business Continuity (BC)

From the results in Table 31 it is clear that, the item 'Existing Business Continuity and Disaster Recovery plans are sufficient to ensure business continuity' is significantly correlated to 'A Business Continuity and Disaster Recovery plan exists', $r(153)= .815$, 'Relevant staff are trained to activate the Business

Continuity and Disaster Recovery plan', $r(153)= .834$, and 'Business Continuity and Disaster Recovery plans are based on international standards', $r(153)= .860$, (all $p < 0.01$).

Table 31 Correlations for Business Continuity Factor

		BC1	BC2	BC3	BC4
BC1	A Business Continuity and Disaster Recovery plan exists	1	.830**	.809**	.815**
BC2	Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan		1	.840**	.834**
BC3	Business Continuity and Disaster Recovery plans are based on international standards			1	.860**
BC4	Existing Business Continuity and Disaster Recovery plans are sufficient to ensure business continuity				1

**. Correlation is significant at the 0.01 level (2-tailed).

6.2.2 Reliability of the Instrument

Reliability denotes that the score from a measurement scale is consistent and stable (Anastasi & Urbina, 1997). Reliability can be conveyed in the form of a correlation coefficient (r), which specifies the degree of the relationship between scores (Dyba, 2000). The value of r ranges between 0 and 1, with 1 indicating perfectly reliable and 0 indicating perfectly unreliable.

Table 32 Summary of Reliability Tests (adapted from (Dyba, 2000))

	Number of Scale Forms	
Number of Administrations	**One**	**Two**
One	Split-Halves	Alternate-Form (immediate)
	Internal Consistency	
Two	Test-Retest	Alternate-Form (delayed)

Dyba (2000) summarises the possible reliability methods based on the number of administrations and scale forms required (see Table 32). The test-retest method involves administering the same scale on the same group of respondents on two different occasions. This will be difficult to implement in a study such as this where the sample size is large and the target respondents are

very specific group such as IT employees in the public sector. The alternate-form method requires administering two equivalent versions of the scale on the same group, either immediately or at a later date. These methods also suffer from the weaknesses of the test-retest method for a study such as the current one. The split-halves method only requires one administration of the scale; however, its limitation arises from the problem of how to split the tests to achieve the most equivalent halves as the estimate of the reliability coefficient totally depends on how the items are split.

This study applied Cronbach's Alpha, which is an internal consistency reliability test that overcomes the shortcomings of the other tests. This test indicates the degree to which items in a scale are consistent. The results obtained with Cronbach Alpha range between 0 and 1. Coefficient alpha is equal to 1 when all the items are perfectly reliable and are measuring the same construct. Table 33 Shows the rules for describing the results of Cronbach's Alpha.

Table 33 Description of Cronbach Alpha Results (DeVellis, 2012)

Cronbach alpha	Level of Internal Consistency
$0.9 \leq \alpha$	Excellent
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Acceptable
$0.6 \leq \alpha < 0.7$	Questionable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

An internal consistency analysis using Cronbach's Alpha was performed on each of the factors in the Government Cloud Readiness Measure. SPSS software was used to calculate Cronbach's Alpha. The results are highlighted in the following section.

6.2.2.1 Internal Consistency for Cloud Readiness Factors

Internal consistency reliability confirmation is a stepwise process. First, reliability is investigated for each factor and if the score is low ($\alpha < 0.7$), items are explored to identify any items that the deletion of will increase the reliability

score. Then, items with low item-item and item-scale scores are considered for elimination if it will improve the value of alpha.

Although, the overall Cronbach's α result of 0.989 shown in Table 34 indicates excellent internal consistency for the instrument, an item was deleted from the Policy and Legislation factor to improve the value of alpha. Table 35 shows that after removing item PL1, the values of α for the factors range between 0.951 and 0.805. These levels indicate a good level of internal consistency.

Table 34 Total Reliability for Instrument

Cronbach's Alpha	N of Items
.989	72

Table 35 Reliability for all Factors

Factor	Number of items	Cronbach's alpha	Items deleted	Cronbach's alpha after deletion
Security	7	0.909	None	
Privacy	4	0.805	None	
Reliability	5	0.886	None	
Leadership	3	0.891	None	
Project Planning	5	0.882	None	
Clear Requirements	4	0.843	None	
Top Management Support	5	0.903	None	
Policy & Legislation	3	0.692	PL1	0.851
Consultant Competency	5	0.922	None	
Cooperation	3	0.927	None	
Coordination	4	0.947	None	
BPR	5	0.954	None	
Communication	3	0.822	None	
Standards	3	0.935	None	
Training	6	0.925	None	
Knowledge Management	3	0.933	None	
Business Continuity	4	0.951	None	

6.2.2.2 Internal Consistency for Security Factor

Although, Table 37shows that deleting item Sec1 will increase the result for Cronbach's α for the Security factor to α= 0.932, no items are deleted. Since the overall reliability for Security factor in Table 36 is excellent with α= 0.909 and only factors with α < 0.7 are considered for item deletion.

Table 36 Reliability for Security Factor

Cronbach's Alpha	N of Items
.909	7

Table 37 Item-Total Statistics for Security Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Sec1	16.88	49.431	.198	.932
Sec2	15.79	37.315	.802	.886
Sec3	15.77	38.167	.867	.882
Sec4	15.03	39.405	.680	.900
Sec5	15.36	36.312	.853	.880
Sec6	14.74	33.475	.793	.891
Sec7	15.36	35.125	.853	.880

6.2.2.3 Reliability for Privacy Factor

From Table 39it is clear that deleting item Prv1 will increase the value of Cronbach's α from 0.805 to 0.882, but this was not deemed necessary since the overall score of Cronbach's α= 0.805 is good.

Table 38 Reliability for Privacy Factor

Cronbach's Alpha	N of Items
.805	4

Table 39 Item-Total Statistics for Privacy Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Prv1	8.57	12.247	.258	.882
Prv2	7.55	7.503	.841	.644
Prv3	6.95	7.851	.721	.704
Prv4	7.01	6.586	.724	.710

6.2.2.4 Reliability for Reliability Factor

The overall reliability shown in Table 40 for the Reliability factor in Cronbach's α= 0.886. Since this score is good none off the items were removed despite the fact that removing Rel1 gives a higher score.

Table 40 Reliability for Reliability Factor

Cronbach's Alpha	N of Items
.886	5

Table 41 Item-Total Statistics for Reliability Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Rel1	10.70	29.760	.212	.943
Rel2	9.44	19.901	.867	.828
Rel3	9.42	19.579	.862	.828
Rel4	9.46	19.076	.812	.841
Rel5	9.70	18.531	.869	.825

6.2.2.5 Reliability for Leadership Factor

Although Table 43 shows that deleting the item Led1 will improve the score for Cronbach's α, the increase was not significant enough to remove the item. Thus, no items were removed and the overall score for Cronbach's α= 0.891 is good.

Table 42 Reliability for Leadership Factor

Cronbach's Alpha	N of Items
.891	3

Table 43 Item-Total Statistics for Leadership Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Led1	5.15	4.050	.720	.903
Led2	4.97	3.377	.836	.801
Led3	4.86	3.021	.826	.815

6.2.2.6 Reliability for Project Planning Factor

The overall score shown in Table 44 of Cronbach's α= 0.882 is good. Thus, it was not deemed necessary to delete any items even if deleting item PP1 will increase the score.

Table 44 Reliability for Project Planning Factor

Cronbach's Alpha	N of Items
.882	5

Table 45 Item-Total Statistics for Project Planning Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PP1	10.09	15.266	.402	.917
PP2	9.46	11.290	.759	.847
PP3	9.51	11.652	.842	.826
PP4	9.75	12.186	.767	.844
PP5	9.66	11.718	.832	.828

6.2.2.7 Reliability for Clear Requirements Factor

The overall result of Cronbach's α= 0.843 shown in Table 46 is good. Hence, no items were deleted.

Table 46 Reliability for Clear Requirements Factor

Cronbach's Alpha	N of Items
.843	4

Table 47 Item-Total Statistics for Clear Requirements Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
ClReq1	7.13	7.559	.480	.882
ClReq2	6.78	6.727	.704	.791
ClReq3	6.51	6.278	.753	.767
ClReq4	6.54	6.091	.795	.747

6.2.2.8 Reliability for Top Management Support Factor

No items were deleted for the Top Management Support Factor since the result shown in Table 48 of Cronbach's α= 0.903 is excellent.

Table 48 Reliability for Top Management Support Factor

Cronbach's Alpha	N of Items
.903	5

Table 49 Item-Total Statistics for Top Management Support

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
TM1	10.80	15.948	.676	.898
TM2	10.32	14.167	.849	.863
TM3	10.33	13.533	.827	.865
TM4	10.20	15.404	.699	.893
TM5	9.82	12.743	.775	.883

6.2.2.9 Reliability for Policy & Legislation Factor

Table 50 displays Cronbach's α= 0.692 which denotes questionable reliability for the Policy and Legislation Factor. Consequently, factor items are considered

for deletion to improve the score. From Table 51, deleting the item PL1 improves the score to good with Cronbach's α= 0.851 and Table 22 highlights that PL1 only has weak to moderate correlations with other factor items. Thus, item PL1is deemed appropriate for deletion.

Table 50 Reliability for Policy & Legislation Factor

Cronbach's Alpha	N of Items
.692	3

Table 51 Item-Total Statistics for Policy & Legislation Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
PL1	5.05	4.649	.279	.851
PL2	3.91	2.737	.699	.314
PL3	4.39	3.487	.595	.489

6.2.2.10 Reliability for Consultant Competency Factor

Since Table 52 displays an excellent reliability score for Consultant Competency factor, Cronbach's α= 0.922, no items were deleted.

Table 52 Reliability for Consultant Competency Factor

Cronbach's Alpha	N of Items
.922	5

Table 53 Item-Total Statistics for Consultant Competency Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
CC1	10.14	15.952	.718	.921
CC2	9.95	12.879	.843	.898
CC3	10.09	15.064	.775	.910
CC4	10.04	13.813	.862	.892
CC5	10.01	14.391	.819	.901

6.2.2.11 Reliability for Cooperation Factor

From Table 54, it is clear that Cooperation has an excellent reliability score of Cronbach's α= 0.927. Thus, it is not necessary to remove any items.

Table 54 Reliability for Cooperation Factor

Cronbach's Alpha	N of Items
.927	3

Table 55 Item-Total Statistics for Cooperation Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Coop1	5.52	6.225	.860	.890
Coop2	5.34	6.068	.836	.908
Coop3	5.16	5.651	.863	.887

6.2.2.12 Reliability for Coordination Factor

The result shown in Table 56 of Cronbach's α= 0.947 for the Coordination factor is excellent. Thus, none of the items were removed.

Table 56 Reliability for Coordination Factor

Cronbach's Alpha	N of Items
.947	4

Table 57 Item-Total Statistics for Coordination Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Coor1	8.54	14.921	.870	.932
Coor2	8.51	14.278	.903	.922
Coor3	8.42	14.245	.823	.949
Coor4	8.39	14.595	.904	.922

6.2.2.13 Reliability for BPR Factor

Table 58 displays an excellent Cronbach's α= 0.954 for the BPR factor. Hence, no items were removed.

Table 58 Reliability for BPR Factor

Cronbach's Alpha	N of Items
.954	5

Table 59 Item-Total Statistics for BPR Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
BPR1	11.09	22.217	.822	.951
BPR2	10.86	21.418	.886	.940
BPR3	10.96	21.932	.929	.934
BPR4	10.66	22.158	.837	.949
BPR5	10.92	22.153	.890	.940

6.2.2.14 Reliability for Communication Factor

Table 60 shows Cronbach's α= 0.822 for the Communication factor. Since this score is good, no items were deleted.

Table 60 Reliability for Communication Factor

Cronbach's Alpha	N of Items
.822	3

Table 61 Item-Total Statistics for Communication Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Com1	5.30	4.514	.532	.885
Com2	4.48	3.133	.727	.709
Com3	4.61	3.608	.805	.630

6.2.2.15 Reliability for Standards Factor

Cronbach's α= 0.935 for the Standards factor presented in Table 62 is an excellent reliability score. Thus, no items were removed.

Table 62 Reliability for Standards Factor

Cronbach's Alpha	N of Items
.935	3

Table 63 Item-Total Statistics for Standards Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Std1	5.49	6.092	.896	.887
Std2	5.64	6.846	.856	.912
Std3	5.74	7.889	.872	.913

6.2.2.16 Reliability for Training Factor

No items were removed for the Training factor since a Cronbach's α= 0.925 shown in Table 64 is excellent.

Table 64 Reliability for Training Factor

Cronbach's Alpha	N of Items
.925	6

Table 65 Item-Total Statistics for Training Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Trn1	11.94	22.718	.756	.915
Trn2	12.18	23.131	.744	.917
Trn3	12.26	23.225	.752	.916
Trn4	11.93	21.498	.844	.903
Trn5	11.78	21.231	.845	.903
Trn6	12.01	22.821	.764	.914

6.2.2.17 Reliability for Knowledge Management Factor

The Cronbach's α= 0.933 for Knowledge Management factor shown in Table 66 is excellent. Hence, no items were deleted.

Table 66 Reliability for Knowledge Management Factor

Cronbach's Alpha	N of Items
.933	3

Table 67 Item-Total Statistics for Knowledge Management Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
KM1	5.11	5.842	.876	.892
KM2	5.18	6.054	.858	.907
KM3	4.92	5.687	.854	.911

6.2.2.18 Reliability of Business Continuity Factor

The Cronbach's α= 0.951 shown in Table 69 is considered an excellent value. Therefore, no items were deleted.

Table 68 Reliability for Business Continuity Factor

Cronbach's Alpha	N of Items
.951	4

Table 69 Item-Total Statistics for Business Continuity Factor

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
BC1	8.62	16.502	.865	.940
BC2	8.22	16.025	.887	.934
BC3	8.13	16.830	.888	.933
BC4	8.17	17.600	.889	.934

6.2.3 Discussion of Validation Results

The Government Cloud Readiness measure was validated in two steps. First, an expert review was conducted to confirm content validity. Then, a pilot study was conducted to examine the strength of the relationships between factors and items and to investigate reliability of the instrument.

Content validity was asserted by having experts review versions in a stepwise process. Experts evaluated updated versions of the instrument until agreement was reached. Consensus was reached on the third version of the instrument that now comprised 72 items instead of 85.

A correlation analysis was performed to investigate the strength of the relationships between the factors, the items and the instrument as a whole. The results display that there are significant relationships among the factors and the items in each factor. These results suggest moderate to strong correlations. Therefore, the instrument is deemed to measure the underlying concept of the FISGC framework.

The internal consistency method was used to examine the reliability of the instrument. Internal consistency was explored for the instrument a whole, each factor and the factor items. The results showed that the overall reliability score

for the instrument is excellent and for the factors, after removing item PL1, is good.

Therefore, the final version of the instrument with 71 items is concluded to be valid and reliable. In the following section the results of applying the instrument to measure Saudi government organisations' cloud readiness are presented.

6.3 Application

In this section the Government Cloud Readiness measure is used to assess the level of government organisations preparedness to implement a private cloud. The instrument is composed of 71 items for measuring fifteen factors. The questions are displayed in Appendix I. While, responses are scores from 5 to 1, with 5 indicating "Always", 4 indicating "Often", 3 indicating "Rarely", 2 indicating "Often" and 1 indicating "Never". "Never" is the lowest possible score and implies almost no existence or compliance of the item in the organisation. On the opposite end, "Always" is the highest possible score and represents the existence or compliance of the item in the organisation. See Table 70. The actual level of compliance with each factor is represented by the average of the item ratings for that factor. These sums are called 'Scale scores'. A government organization's chances of success with its cloud implementation program can be predicted via a vector of the scale scores for the fifteen factors.

Table 70 Overview Response Scores

Response	Definition
1 Never	The item shows non readiness/compliance with corresponding factor
2 Rarely	The item shows minor readiness /compliance with corresponding factor
3 Sometimes	The item shows acceptable readiness/compliance with corresponding factor
4 Often	The item shows satisfactory readiness/compliance with corresponding factor
5 Always	The item shows ideal readiness/compliance with corresponding factor

A sample of 167 IT employees working in Saudi government organizations completed the instrument. Their responses are used to understand the state Saudi government's readiness for implementing a private cloud. The results are presented in

Table 71. The overall score of 2.53 indicates only minor readiness. Figure 11 compares the readiness scores for factors. It shows Security and Privacy having the highest score with 3.1 and Clear Requirements having the lowest score with 2.21. All factors, except for Security and Privacy that shows acceptable readiness, show minor readiness.

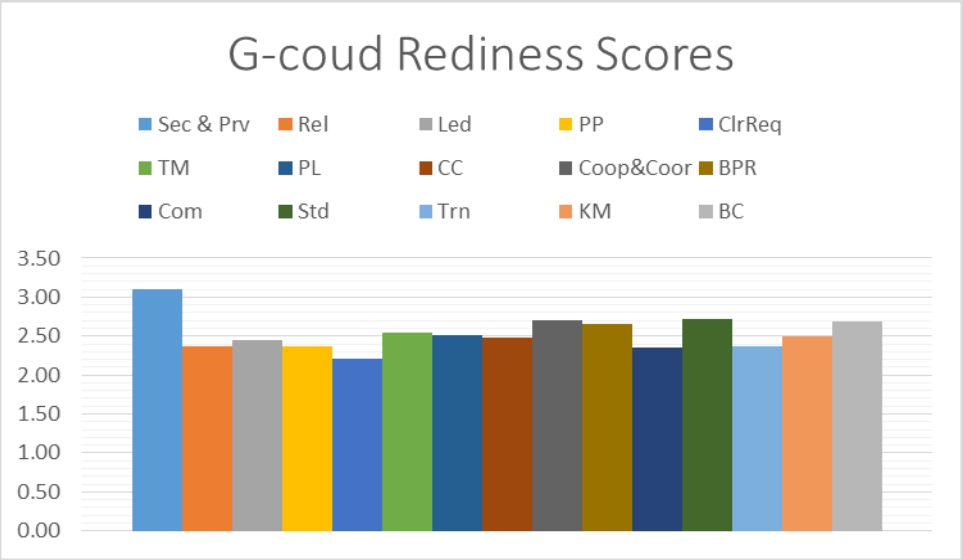

Figure 11 Readiness Scores for Factors

Table 71 Readiness Scores

Factor	Max Score	Actual Score
Security and Privacy	5	3.10
Reliability	5	2.37
Leadership	5	2.45

Project Planning	5	2.37
Clear Requirements	5	2.21
Top Management Support	5	2.54
Policy and Legislation	5	2.52
Consultant Competence	5	2.48
Cooperation and Coordination	5	2.71
BPR	5	2.65
Communication	5	2.36
Standards	5	2.72
Training	5	2.37
Knowledge Management	5	2.50
Business Continuity	5	2.69
Overall	5	2.53

The measure can be used to identify relevant items from each factor to develop with the goal of improving overall readiness. An example is given of the Clear Requirement scores in Table 73. The item scores show no to minor readiness. So focusing on complying with these items will improve the readiness score for Clear Requirements. Thus, improving overall readiness. The items are defined in Table 72

Table 72 Definition of Clear Requirement items

ClReq1	Requirements gathering is an important stage
ClReq2	A formalised process is followed
ClReq3	Project requirements are clear
ClReq4	Requirement gathering is done effectively

Table 73 Readiness Scores for ClReq

ClReq1	ClReq2	ClReq3	ClReq4
1.83	2.16	2.44	2.39

6.4 Chapter Summary

This chapter described the validation process for the Government Cloud Readiness measure developed in Chapter 5: First, content validity was established via an expert review that confirmed 72 items. Then, correlation analysis was performed to establish the relationships among factors and items. The results suggested that the instrument was able to measure the underlying construct of the FSIGC. Finally, an internal consistency test was conducted to confirm reliability of the instrument. The results showed that the factors and 71 items have good internal consistency. Thus, the Government Cloud Readiness Measure was deemed valid and reliable. Following that, it was used to measure government cloud readiness in Saudi government agencies.

Chapter 7: Conclusion

This chapter gives an overview of the research conducted in 8.1 . Then, the contributions made are highlighted in 8.2. After that, limitations of this research are pointed out in 8.3. The chapter is concluded with suggested directions for future work in 8.4.

7.1 Research Overview

The government of Saudi Arabia is in the process of transitioning to e-government. This transition is hindered by the weakness of ICT infrastructure in Saudi government agencies. The development of a private government cloud is a solution for rapidly improving the ICT infrastructure.

The purpose of this research was to develop a framework for successful implementation of a private government cloud in Saudi Arabia. A qualitative review of the literature has shown that there are several challenges that need to be overcome when developing a private cloud for intergovernmental interaction in Saudi Arabia. By identifying the challenges, it was possible to determine ten success factors for the implementation of a private government cloud in Saudi Arabia. The FSIGC framework is described in Chapter 4 of this thesis was constructed based on reviewing relevant literature and synthesising the findings. The ten identified success factors are:

1. Security and Privacy
2. Reliability
3. Cooperation and Coordination
4. Policy and Legislation
5. Leadership
6. Business Process Re-Engineering
7. Project planning
8. Clear requirements

9. Top management support

10. Consultant competence

A mixed method triangulation approach was used to validate the framework. The methods used included an expert review of twelve IT experts in Saudi government agencies and a survey of thirty Saudi government IT employees. The expert review confirmed the importance of the proposed ten factors and identified five further factors. These factors were confirmed via the questionnaire survey. The additional five factors that emerged from the evaluation study, shown in Chapter 5 are:

1. Communication

2. Standards

3. Knowledge Management

4. Training

5. Business Continuity

The fifteen factor FSIGC was used as a reference to build the Government Cloud Reediness Measure. The Government Cloud Readiness Measure is an instrument that measures to what extent government organisations are complying with FSIGC. Items were generated to represent the factors in FSIGC based on a literature review. The constructed instrument was comprised of 85 items to represent 15 factors. Next, an expert review with eleven IT experts from Saudi government agencies was conducted to confirm the content validity of the instrument. The content valid instrument was comprised of 72 items representing 15 factors as the experts recommended splitting the Security and Privacy component. After that, a pilot study which involved an online survey which was completed by 153 Saudi IT government employees. The first aim of the pilot study, was to explore the relationships between the factors and the instrument as a whole, and the items in each factor. Correlation analysis was used for this. Results of the analysis suggest that the Government Cloud Readiness Measure has statistically significant correlations between items and factors and towards the instrument as a whole. The second aim of the pilot

study, was to investigate reliability of the instrument. Results of the internal consistency reliability analysis showed that instrument has good internal consistency after removing one item. The refined instrument is comprised of 71 items. These results suggest that Government Cloud Readiness Measure is valid and has the required level of reliability.

The aim of this research is to answer two research questions:

RQ1: What framework will lead to the successful implementation of a private government cloud in Saudi Arabia?

RQ2: Are the proposed success factors being employed in Saudi government agencies ??

To help determine the factors that affect the implementation of a private government cloud in Saudi Arabia, government IT experts' opinions were elicited. RQ1 was divided into the following sub-questions:

RQ1.1: What are the factors that pose challenges to the implementation of a private government cloud in Saudi Arabia?

RQ1.2: How can these factors be validated? The two sub-questions (RQ1.1 and RQ1.2) were answered in Chapters 2-4 of this thesis. The study identified both challenges and success factors, which were then used to construct a framework for the successful implementation of a private government cloud in Saudi Arabia.

The second research question's aim was to develop and validate an instrument for assessing the readiness of Saudi government agencies for the implementation of a private government cloud. This question was answered in Chapter 6 and 7 of this thesis. The Government Cloud Readiness Measure was developed from a desk based study. After which, an expert review and statistical study were conducted to validate the instrument and ensure its reliability. Following that it was used to assess the level of cloud readiness in Saudi government agencies which highlighted that these agencies are still unprepared for cloud implementation. The factors and corresponding items identified in this research may be used as guidelines for improving readiness.

7.2 Contribution

This research is one of a few studies investigating critical success factors for the implementation of cloud computing. It focused on the implementation of cloud computing in the unique environment of Saudi Arabian government agencies. This is significant as methods implemented in the private sector or in other countries may not be effective for the successful implementation of cloud computing for e-government in Saudi Arabia. The main contributions of this study can be described as follows:

The key factors that may affect the successful implementation of cloud computing Saudi Arabian government organisations were identified. To the author's knowledge this is the only study to tackle this gap in the research.

The main contribution of this study was the developed framework for the successful implementation of cloud computing in Saudi government. The framework was constructed from a comprehensive literature review and interviewing Saudi Arabian IT and cloud computing experts. This helped identify the factors unique to Saudi government organizations that had not been previously identified in the literature.

Specific items were identified to represent each of the success factors. These items may serve as implementation guidelines for cloud computing in Saudi government organizations. This contribution aids in bridging the gap between theory and practice.

An exploratory approach based on widely accepted methodologies was used to develop an instrument to assess government organisation's readiness to implement cloud computing. This instrument is a practical tool for government IT managers to plan their cloud computing projects.

The factors and items identified in this study can be used as a basis for other developing countries that are in the process of starting their government cloud initiatives.

7.3 Research Limitations

While this research successfully achieved its objectives, understanding the critical success factors for implementing cloud computing in Saudi Arabia where there was a lack of related studies was challenging. Hence, identification of the key success factors is mostly based on the perceptions of interviewed experts.

A limitation comes from the diversity in the nature of the participating government and semi-government organizations, which ranged from military, healthcare, and financial institutions where security and privacy should be extremely important, to government departments for sports and entertainment, and media, where those factors may not be as important. While this diversity aids in gaining a clear understanding of the overall critical success factors, by nature some organizations will prioritize certain factors while others will not.

Another limitation for this study is that the findings cannot be generalized beyond Saudi Arabia where it was conducted. Nonetheless, the findings can be used as a basis for studies in other countries and other types of organizations.

In addition, the data gathered was based on the input of employee responses to interviews and surveys related to their perceptions of the performance of their organizations; employees may, from loyalty, dissatisfaction, or fear of reprisal, deliberately or subconsciously misrepresent their organizations' performance.

7.4 Future Work

This research was designed to investigate the factors affecting the successful implementation of cloud computing in Saudi Arabian government agencies. The next phase of research would involve ranking the items representing the factors based on their importance and identifying any relationships between these items. Following that, it would be beneficial to empirically validate the developed instrument via case studies. Case studies would aid in assessing the value added to government cloud implementation plans from utilising the instrument, thereby transitioning from theoretical to practical application of the framework. Having before and after implementation surveys would give an in-depth understanding of the entire implementation process for cloud adoption, and in the future the adoption of other IT technology.

Another avenue for investigation would be to use this study as a basis for investigation into other countries/regions and non-government organisations. These can then be used in comparison studies to identify the differences between them. In addition, future research should include the perspectives of other stakeholders including top managers, external IS consultants, and cloud providers.

Appendix A Interview Questions

1) In the table, some factors for the successful implementation of a private government cloud are proposed. Please state whether you find the proposed factor important or not.

Factor	Important	unnecessary/ impractical	Reason for Choice
Security & Privacy			
Reliability			
Leadership			
Project Planning			
Clear Statement of Requirements			
Top Management Support			
Policy and Legislation			
Consultant Competency (skills)			
Cooperation and Coordination			
Business Process Re-Engineering			

2) What other factors do you recommend to ensure the successful implementation of a private G-cloud?

3) Does your organization use/ *have used in the past* cloud computing? *If No, go to Q 9*

4) What type of cloud? (Public, Private or Hybrid)

5) What do you use the cloud for?

6) Are you satisfied with the services provided by the cloud?

7) Why are you satisfied/ dissatisfied?

8) What challenges did you face when implementing your cloud service?

9) What is stopping you from using cloud computing?

Appendix B Survey

Part 1:

1) Have you worked on an IT project for a government organization? (For example building, designing or installing a new computerized system)
   - Yes
   - No
2) What is the classification of your Organization?
   - Government
   - Semi-government
   - Private
3) Choose the option that best reflects your years of experience
   - Less than 2 years
   - 2 – 5 years
   - 6 – 10 years
   - More than 10 years

Part 2:

No	**To what extent do you agree that the following factors are important to the *successful* implementation of a private government cloud in Saudi Arabia?**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
1	The developed private cloud must be secure.					
2	The developed private cloud must guarantee privacy.					
3	The developed private cloud must be reliable.					
4	Changes must be made in governmental policies to ensure the safety of all stakeholders in a private government cloud.					
5	Standards governing information exchange between the different government entities must be improved.					
6	Knowledge management must be undertaken throughout the lifecycle of the project.					
7	Cooperation between the various stakeholders is required.					
8	Technical coordination is required to ensure interoperability.					
9	Transparency throughout all stages of the implementation.					

No	To what extent do you agree that the following factors are important to the *successful* implementation of a private government cloud in Saudi Arabia?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
10	Giving regular updates and sharing information about the progress of the project.					
11	Business Process Re-Engineering is necessary.					
12	Training must be provided for technical staff.					
13	Training must be provided to end-users.					
14	Top management support is essential.					
15	The requirements must be stated and communicated clearly to the development team.					
16	Proper planning is vital.					
17	A project leader must be appointed to maintain all the information on the project and to coordinate between the different stakeholders.					
18	IT consultants must have appropriate skills and knowledge.					
19	Business continuity must be considered.					
20	Disaster recovery must be considered.					

Appendix C Instrument V1

Part 1:

1) Have you worked on an IT project for a government organization? (For example building, designing or installing a new computerized system)
   - Yes
   - No
2) What is the classification of your Organization?
   - Government
   - Semi-government
   - Private
3) Choose the option that best reflects your years of experience
   - Less than 2 years
   - 2 – 5 years
   - 6 – 10 years
   - More than 10 years

Part 2:

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Security and Privacy	1	IS security and privacy are given high priority.					
	2	A person/ department is appointed to manage security and privacy.					
	3	IS security and privacy is managed effectively.					
	4	IS security and privacy training is provided for employees.					
	5	Specific IS security requirements are applied.					
	6	These requirements are standard-based.					
	7	These requirements are formalized in a policy document.					
	8	Specific privacy laws/regulations are followed.					
	9	International transfer of data is limited.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Reliability	10	IS reliability is given priority.					
	11	A person/ department is appointed to manage IS reliability.					
	12	I can count on information systems being available when I need them.					
	13	IS reliability is monitored.					
	14	Unreliable IS are changed/fixed.					
	15	Limits are set on acceptable system downtime.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Leadership	16	Project managers are supported.					
	17	A project manager is designated for IS projects.					
	18	The project manager assigned is the best person for the job.					
	19	The project manager has a positive effect on project success.					
	20	The project team is happy to follow the PM.					
	21	Project managers are assigned based on specific requirements.					
	22	Training is provided for project managers.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Project Planning	23	Project planning is important.					
	24	A formal project plan is established before an IS project is started.					
	25	Project scopes are carefully defined.					
	26	A project team is designated for IS projects.					
	27	Realistic deadlines and budget are set.					
	28	Regular project status meetings are scheduled.					
	29	Project plans are effective.					
	30	Training is provided on developing project plans.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Clear Requirements	31	Requirements gathering is an important stage in IS projects.					
	32	Formal methods are used for gathering requirements.					
	33	IS project requirements are clear and complete.					
	34	Requirement gathering is done effectively.					
Top Management Support	35	Top management champion IS projects.					
	36	Top management provides projects with necessary resources.					
	37	Top management continuously monitor projects throughout their lifecycle.					
	38	Top management provide leadership for the project team.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Policy and Legislation	39	There are existing local government legislations and policies that cover cloud computing.					
	40	These legislation and policies are sufficient.					
	41	These legislation and policies are effective.					
	42	Our organization has the competencies necessary to comply with these policies and legislations.					
Consultant competency	43	External IS consultants are given support.					
	44	We have formal processes for hiring/ (validating) external IS consultants.					
	45	External IS consultants are competent.					
	46	They have a positive effect on the success of IS projects.					
	47	External consultants are important to IS projects.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Cooperation	48	Cooperation is encouraged between all stakeholders in IS projects.					
	49	Cooperation between IS project stakeholders is formalized.					
	50	Cooperation is successful.					
	51	Cooperation between IS stakeholders is facilitated in our organization.					
Coordination	52	Coordination of legacy systems with new IS is supported.					
	53	New systems are integrated with partner organization's systems.					
	54	Formal processes are followed for coordination.					
	55	Someone is assigned to manage coordination.					
	56	Coordination is successful.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Business Process Re-engineering (BPR)	57	Business processes are adapted to fit new systems.					
	58	A team is assigned to implement BPR.					
	59	Formal BPR strategies exist.					
	60	Enough time and resources are allocated to BPR.					
	61	BPR is effective.					
	62	Staff is trained on new business processes.					
Communication	63	Communication is a priority.					
	64	We have a clear communication plan.					
	65	Communication is effective.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Standards	66	Standards for exchanging information exist.					
	67	These standards are managed by a person/group.					
	68	A formal repository for information exchange is available.					
	69	Information exchange is successful.					
	70	Training is provided on information exchange standards.					
Training	71	Training for new systems is given priority.					
	72	When new systems are introduced, the training provided is adequate in length and detail.					
	73	The training improves the level of users' understanding.					
	74	The training gives users' confidence in the new system.					
	75	The training is handled by knowledgeable and competent trainers.					

Factor	No	To what extent do you agree that these statements are true about your organization?	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Knowledge Management	76	Knowledge sharing is supported.					
	77	Specific techniques and strategies are used for sharing knowledge.					
	78	Technology is used for sharing knowledge.					
	79	Training is provided on knowledge sharing.					
	80	Strict documentation laws are employed.					
Business Continuity	81	A Business Continuity and Disaster Recovery plan exists.					
	82	Someone is responsible for Business continuity management.					
	83	The Business continuity plan is regularly reviewed and updated.					
	84	Business Continuity and Disaster Recovery procedures are documented.					
	85	Relevant staff is trained to activate the Business Continuity and Disaster Recovery plan.					

Appendix D Instrument V1 Expert Review

Part 1: Please state whether the selected items are adequate and relevant to the factor they represent

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Security and Privacy	1	IS security and privacy are given high priority.		
	2	A person/ department is appointed to manage security and privacy.		
	3	IS security and privacy is managed effectively.		
	4	IS security and privacy training is provided for employees.		
	5	Specific IS security requirements are applied.		
	6	These requirements are standard-based.		
	7	These requirements are formalized in a policy document.		
	8	Specific privacy laws/regulations are followed.		
	9	International transfer of data is limited.		
Are these items adequate to represent *Security and Privacy*?				
Can you suggest additional items to represent *Security and Privacy*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Reliability	10	IS reliability is given priority.		
	11	A person/ department is appointed to manage IS reliability.		
	12	I can count on information systems being available when I need them.		
	13	IS reliability is monitored.		
	14	Unreliable IS are changed/fixed.		
	15	Limits are set on acceptable system downtime.		
Are these items adequate to represent *Reliability*?				
Can you suggest additional items to represent *Reliability*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Leadership	16	Project managers are supported.		
	17	A project manager is designated for IS projects.		
	18	The project manager assigned is the best person for the job.		
	19	The project manager has a positive effect on project success.		
	20	The project team is happy to follow the PM.		
	21	Project managers are assigned based on specific requirements.		
	22	Training is provided for project managers.		
Are these items adequate to represent *Leadership*?				
Can you suggest additional items to represent *Leadership*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Project Planning	23	Project planning is important.		
	24	A formal project plan is established before an IS project is started.		
	25	Project scopes are carefully defined.		
	26	A project team is designated for IS projects.		
	27	Realistic deadlines and budget are set.		
	28	Regular project status meetings are scheduled.		
	29	Project plans are effective.		
	30	Training is provided on developing project plans.		
Are these items adequate to represent *Project Planning*?				
Can you suggest additional items to represent *Project Planning*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Clear requirements	31	Requirements gathering is an important stage in IS projects.		
	32	Formal methods are used for gathering requirements.		
	33	IS project requirements are clear and complete.		
	34	Requirement gathering is done effectively.		
Are these items adequate to represent *Clear statement of requirements*?				
Can you suggest additional items to represent *Clear statement of requirements*?				
Top management support	35	Top management champion IS projects.		
	36	Top management provides projects with necessary resources.		
	37	Top management continuously monitor projects throughout their lifecycle.		
	38	Top management provide leadership for the project team.		

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Are these items adequate to represent *Top management support*?				
Can you suggest additional items to represent *Top management support*?				
Policy and legislation	39	There are existing local government legislations and policies that cover cloud computing.		
	40	These legislation and policies are sufficient.		
	41	These legislation and policies are effective.		
	42	Our organization has the competencies necessary to comply with these policies and legislations.		
Are these items adequate to represent *Policy and Legislation*?				
Can you suggest additional items to represent *Policy and Legislation*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Consultant competency	43	External IS consultants are given support.		
	44	We have formal processes for hiring/ (validating) external IS consultants.		
	45	External IS consultants are competent.		
	46	They have a positive effect on the success of IS projects.		
	47	External consultants are important to IS projects.		
Are these items adequate to represent *Consultant competency*?				
Can you suggest additional items to represent *Consultant competency*?				
Cooperation	48	Cooperation is encouraged between all stakeholders in IS projects.		
	49	Cooperation between IS project stakeholders is formalized.		
	50	Cooperation is successful.		
	51	Cooperation between IS stakeholders is facilitated in our organization.		

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Are these items adequate to represent *Cooperation*?				
Can you suggest additional items to represent *Cooperation*?				
Coordination	52	Coordination of legacy systems with new IS is supported.		
	53	New systems are integrated with partner organization's systems.		
	54	Formal processes are followed for coordination.		
	55	Someone is assigned to manage coordination.		
	56	Coordination is successful.		
Are these items adequate to represent *Coordination*?				
Can you suggest additional items to represent *Coordination*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Business Process Re-engineering (BPR)	57	Business processes are adapted to fit new systems.		
	58	A team is assigned to implement BPR.		
	59	Formal BPR strategies exist.		
	60	Enough time and resources are allocated to BPR.		
	61	BPR is effective.		
	62	Staff are trained on new business processes.		
Are these items adequate to represent *BPR*?				
Can you suggest additional items to represent *BPR*?				
Communication	63	Communication is a priority.		
	64	We have a clear communication plan.		
	65	Communication is effective.		
Are these items adequate to represent *Communication*?				
Can you suggest additional items to represent *Communication*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Standards	66	Standards for exchanging information exist.		
	67	These standards are managed by a person/group.		
	68	A formal repository for information exchange is available.		
	69	Information exchange is successful.		
	70	Training is provided on information exchange standards.		
Are these items adequate to represent *Standards*?				
Can you suggest additional items to represent *Standards*?				

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Training	71	Training for new systems is given priority.		
	72	When new systems are introduced, the training provided is adequate in length and detail.		
	73	The training improves the level of users' understanding.		
	74	The training gives users' confidence in the new system.		
	75	The training is handled by knowledgeable and competent trainers.		
Are these items adequate to represent *Training*?				
Can you suggest additional items to represent *Training*?				
Knowledge Management	76	Knowledge sharing is supported.		
	77	Specific techniques and strategies are used for sharing knowledge.		
	78	Technology is used for sharing knowledge.		
	79	Training is provided on knowledge sharing.		
	80	Strict documentation laws are employed.		

Factor	No	Selected Items	Item is relevant to factor (yes/no)	Comments
Are these items adequate to represent *Knowledge Management*?				
Can you suggest additional items to represent *Knowledge Management*?				
Business Continuity	81	A Business Continuity and Disaster Recovery plan exists.		
	82	Someone is responsible for Business continuity management.		
	83	The Business continuity plan is regularly reviewed and updated.		
	84	Business Continuity and Disaster Recovery procedures are documented.		
	85	Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan.		
Are these items adequate to represent *Business Continuity*?				
Can you suggest additional items to represent *Business Continuity*?				

Part 2: Please answer the following questions about the instrument in general.

No	Question	Agree	Disagree	Comment
1	The wording of the instrument is appropriate.			
2	The responses of the instrument are appropriate.			
3	The layout of the instrument is appropriate.			
4	The length of the instrument is appropriate.			
5	The instrument is easy to read and understand.			

Appendix E Instrument V2

Part 1: Please answer the following questions about yourself and your organisation.

1) Have you worked on an IT project for a government organization? (For example building, designing or installing a new computerized system)
- Yes
- No

2) What is the classification of your Organization?
- Government
- Semi-government
- Private

3) Choose the option that best reflects your years of experience
- Less than 2 years
- 2 – 5 years
- 6 – 10 years
- More than 10 years

Part 2: Please state how frequently the following statements apply to your organisation.

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security	1	Information security is given high priority in my organisation.					
	2	A person/ department is appointed to manage information security policies in my organisation.					
	3	Information security is managed effectively in my organisation.					
	4	Information security training is provided for employees in my organisation.					
	5	International Information security standards are implemented in my organisation(ex. ISO 27001 and ISO 27002).					
	6	International Cloud security standards are implemented in my organisation (ex. ISO 27017 and Cobit Cloud).					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security	7	Information Security standards are formalised and followed in my organisation.					
Privacy	8	Privacy is given high priority in my organisation.					
	9	Privacy is managed effectively in my organisation.					
	10	Information privacy training is provided for employees in my organisation.					
	11	International privacy standards are implemented in my organisation (ex. ISO/IEC 27018).					
Reliability	12	Information system reliability is given priority in my organisation.					
	13	I can count on information systems being continuously available in my organisation.					
	14	Unreliable information systems are immediately repaired or changed in my organisation.					
	15	Maximum acceptable downtime limits are set for each system in my organisation.					
	16	Precaution measures are put in place to avoid information system downtime in my organisation.					
Leadership	17	Top management supports information system project managers in my organisation.					
	18	Qualified project managers are assigned to information system projects in my organisation.					
	19	In the past, project managers contributed to the success of information system projects in my organisation.					
Project Planning	20	Information system project planning is a priority in my organisation.					
	21	A specific project team is assigned to information system in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Project Planning	22	Project plans are effective for the success of information system projects in my organisation.					
	23	Project plans are approved by top management in my organisation.					
	24	Information system project plans are based on international standards in my organization (ex. PRINCE2/PMP).					
Clear statement of requirements	25	Requirements gathering is an important stage for information system projects in my organisation.					
	26	A formalised process is followed for gathering information system requirements in my organisation.					
	27	Information system project requirements are clear in my organisation.					
	28	Information system requirement gathering is done effectively in my organisation.					
Top management support	29	Top management support information system projects in my organisation.					
	30	Top management provides information system projects with necessary resources in my organisation.					
	31	Top management continuously monitor information system projects throughout their lifecycle in my organisation.					
	32	Top management rewards/ penalizes teams working on successful/ failed information system projects in my organisation.					
Policy and legislation	33	There are existing local government legislations and policies that cover cloud computing.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Policy and legislation	34	Existing local government legislation and policies are effective.					
	35	My organization has the competencies necessary to comply with local policies and legislations.					
Consultant competency	36	External information system consultants are given support in my organisation.					
	37	There is a formal process for hiring external information system consultants in my organisation.					
	38	Previous external information system consultants have been competent.					
	39	External information system consultants follow a formal consulting process in my organization.					
	40	External information system consultants are hired based on competency in our organization (i.e. not based on lowest cost).					
Cooperation	41	Cooperation is encouraged between all information system stakeholders in my organisation.					
	42	Cooperation between information system project stakeholders is formalized in my organisation.					
	43	On past information system projects in our organisation, cooperation between stakeholders was successful.					
Coordination	44	Coordination of legacy systems with new information systems is supported in my organisation.					
	45	Coordination of partner organisation's systems with new information systems is supported in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Coordination	46	Personnel are dedicated to oversee coordination of information systems in my organisation.					
	47	In the past, coordination of information systems has been successful in my organisation					
Business Process Re-engineering (BPR)	48	Information systems are adapted to fit new business processes in my organisation.					
	49	BPR strategies are formalised and followed in my organisation.					
	50	Systems are adapted successfully to fit new business processes in my organisation.					
	51	Training is provided for resources when new business processes are introduced in my organisation.					
	52	BPR is aligned with existing processes in my organization.					
Communication	53	A formal communication plan is followed in my organisation.					
	54	Communication plans are updated in my organization.					
	55	In the past communication was effective on information system projects in my organisation.					
Standards	56	Information exchange follows international standards in my organisation.					
	57	A formal repository for information exchange is available in my organisation.					
	58	The exchange of information is effective in my organisation.					
Training	59	Training for new information systems is given priority in my organisation.					
	60	Training improves the level of users' understanding of new information systems in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Training	61	Training gives users' confidence in using new information systems in my organisation.					
	62	Training sessions are taught by qualified professionals in my organisation.					
	63	Training materials are updated in my organization.					
	64	Help desks are available to provide post –training support in my organization.					
Knowledge Management	65	Formal techniques and strategies are used for sharing knowledge in my organisation.					
	66	Technology is utilised for sharing knowledge in my organisation.					
	67	Knowledge sharing is monitored in my organization.					
Business Continuity	68	A Business Continuity and Disaster Recovery plan exists in my organisation.					
	69	Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan in my organisation.					
	70	Business Continuity and Disaster Recovery plans are based on international standards in my organization(ex ISO 22301).					
	71	Existing Business Continuity and Disaster Recovery plans are sufficient to insure business continuity in my organization.					

Appendix F Instrument V3

Part 1: Please answer the following questions about yourself and your organisation.

1) Have you worked on an IT project for a government organization? (For example building, designing or installing a new computerized system)
- Yes
- No
2) What is the classification of your Organization?
- Government
- Semi-government
- Private
3) Choose the option that best reflects your years of experience
- Less than 2 years
- 2 – 5 years
- 6 – 10 years
- More than 10 years
4) What industry does your organisation fall under?
- Health care
- Education
- Military
- Other

Part 2: Please state how frequently the following statements apply to your organisation.

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security	1	Information security is given high priority in my organisation.					
	2	A person/ department is appointed to manage information security policies in my organisation.					
	3	Information security is managed effectively in my organisation.					
	4	Information security training is provided for employees in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security	5	International Information security standards are implemented in my organisation(ex. ISO 27001 and ISO 27002).					
	6	International Cloud security standards are implemented in my organisation (ex. ISO 27017 and Cobit Cloud).					
	7	Information Security standards are formalised and followed in my organisation.					
Privacy	8	Privacy is given high priority in my organisation.					
	9	Privacy is managed effectively in my organisation.					
	10	Information privacy training is provided for employees in my organisation.					
	11	International privacy standards are implemented in my organisation (ex. ISO/IEC 27018).					
Reliability	12	Information system reliability is given priority in my organisation.					
	13	I can count on information systems being continuously available in my organisation.					
	14	Unreliable information systems are immediately repaired or changed in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Reliability	15	Maximum acceptable downtime limits are set for each system in my organisation.					
	16	Precaution measures are put in place to avoid information system downtime in my organisation.					
Leadership	17	Top management supports information system project managers in my organisation.					
	18	Qualified project managers are assigned to information system projects in my organisation.					
	19	In the past, project managers contributed to the success of information system projects in my organisation.					
Project Planning	20	Information system project planning is a priority in my organisation.					
	21	A specific project team is assigned to information system in my organisation.					
	22	Project plans are effective for the success of information system projects in my organisation.					
	23	Project plans are approved by top management in my organisation.					
	24	Information system project plans are based on international standards in my organization (ex. PRINCE2/PMP).					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Clear requirements	25	Requirements gathering is an important stage for information system projects in my organisation.					
	26	A formalised process is followed for gathering information system requirements in my organisation.					
	27	Information system project requirements are clear in my organisation.					
	28	Information system requirement gathering is done effectively in my organisation.					
Top management support	29	Top management support information system projects in my organisation.					
	30	Top management provides information system projects with necessary resources in my organisation.					
	31	Top management continuously monitors information system projects throughout their lifecycle in my organisation.					
	32	Top management rewards/ penalizes teams working on successful/ failed information system projects in my organisation.					
	33	Top management in my organisation understands the benefits of migrating to the cloud.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Policy and legislation	34	There are existing local government legislations and policies that cover cloud computing.					
	35	Existing local government legislation and policies are effective.					
	36	My organization has the competencies necessary to comply with local policies and legislations.					
Consultant competency	37	External information system consultants are given support in my organisation.					
	38	There is a formal process for hiring external information system consultants in my organisation.					
	39	Previous external information system consultants have been competent.					
	40	External information system consultants follow a formal consulting process in my organization.					
	41	External information system consultants are hired based on competency in our organization (i.e. not based on lowest cost).					
Cooperation	42	Cooperation is encouraged between all information system stakeholders in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Cooperation	43	Cooperation between information system project stakeholders is formalized in my organisation.					
	44	On past information system projects in our organisation, cooperation between stakeholders was successful.					
Coordination	45	Coordination of legacy systems with new information systems is supported in my organisation.					
	46	Coordination of partner organisation's systems with new information systems is supported in my organisation.					
	47	Personnel are dedicated to oversee coordination of information systems in my organisation.					
	48	In the past, coordination of information systems has been successful in my organisation.					
Business Process Re-engineering (BPR)	49	Information systems are adapted to fit new business processes in my organisation.					
	50	BPR strategies are formalised and followed in my organisation.					
	51	Systems are adapted successfully to fit new business processes in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Business Process Re-engineering (BPR)	52	Training is provided for resources when new business processes are introduced in my organisation.					
	53	BPR is aligned with existing processes in my organization.					
Communication	54	A formal communication plan is followed in my organisation.					
	55	Communication plans are updated in my organization.					
	56	In the past communication has been effective on information system projects in my organisation.					
Standards	57	Information exchange follows international standards in my organisation.					
	58	A formal repository for information exchange is available in my organisation.					
	59	The exchange of information is effective in my organisation.					
Training	60	Training for new information systems is given priority in my organisation.					
	61	Training improves the level of users' understanding of new information systems in my organisation.					
	62	Training gives users' confidence in using new information systems in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Training	63	Training sessions are taught by qualified professionals in my organisation.					
	64	Training materials are updated in my organisation.					
	65	Help desks are available to provide post – training support in my organisation.					
Knowledge Management	66	Formal techniques and strategies are used for sharing knowledge in my organisation.					
	67	Technology is utilised for sharing knowledge in my organisation.					
	68	Knowledge sharing is monitored in my organisation.					
Business Continuity	69	A Business Continuity and Disaster Recovery plan exists in my organisation.					
	70	Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan in my organisation.					
	71	Business Continuity and Disaster Recovery plans are based on international standards in my organization(ex ISO 22301).					
	72	Existing Business Continuity and Disaster Recovery plans are sufficient to ensure business continuity in my organization.					

Appendix G Participant Information Sheet

Study Title: Investigating factors for ensuring the successful implementation of a private Government cloud in Saudi Arabia

Researcher: Amal Alkhlewi

Ethics number: 9509

Please read this information carefully before deciding to take part in this research. If you are happy to participate you will be asked to sign a consent form.

What is the research about?

This research is required as part of the researcher's PhD degree in computer science. The aim of this research is to investigate factors that influence the successful implementation of a private Government cloud in Saudi Arabia. For the implementation of this research, you will be shown the proposed framework for the successful implementation of a private G-cloud in Saudi Arabia and asked question to help improve the framework.

Why have I been chosen to participate?

You are invited to participate in this study because you are an IT expert working in a Saudi government agency. Your opinion and expertise will help in improving the constructed framework.

What will happen to me if I take part?

I will ask you to sign a consent form, and then the study will begin. I will conduct an interview with you, with open-ended questions, and I will record your voice during the interview.

Are there any benefits in my taking part?

This research is not designed to help you personally, but your feedback will help me gather expert opinions on the development efforts.

Will my participation be confidential?

Yes. Your data and that of other participants will be stored and used on secure systems. Any stored data will not be linked to your name. Any information related to your organization will not be disclosed, the type of organization will be mentioned only.

Are there any risks involved?

No.

What happen if I change my mind?

You have the right to terminate your participation in the research, at any stage, you do not need to give any reasons, and without your legal rights being affected. Any data collected form you will be immediately destroyed.

Where I can get more information?

For further details, please contact either myself or my study supervisors, Dr Robert Walters and Dr Gary Wills.

Amal Alkhlewi: aa3d12@ecs.soton.ac.uk

Dr Robert Walters: rjw1@ecs.soton.ac.uk

Dr Gary Wills: gbw@ecs.soton.ac.uk

Appendix H CONSENT FORM

Study title: Investigating factors for ensuring the successful implementation of a private Government cloud in Saudi Arabia

Researcher name: Amal Alkhlewi

Supervisors: Dr. Robert Walters and Dr. Gary Wills

Ethics reference: 9509

Please initial the box(es) if you agree with the statement(s):

I have read and understood the information sheet and have had the opportunity to ask questions about the study ☐

I agree to take part in this research project and agree for my data to be used for the purpose of this study ☐

I understand my participation is voluntary and I may withdraw at any time without consequence and my data will be deleted if I withdraw at any time ☐

I agree to record my voice during my participation in this study ☐

Data Protection

I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.

Name of participant (print name)…….

Signature of participant…….

Name of Researcher (print name): Amal Alkhlewi

Signature of Researcher……

Date……..

Appendix I Cloud Readiness Measure

Please state how frequently the following statements apply to your organisation.

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security and Privacy	1	Information security is given high priority in my organisation.					
	2	A person/ department is appointed to manage information security policies in my organisation.					
	3	Information security is managed effectively in my organisation.					
	4	Information security training is provided for employees in my organisation.					
	5	International Information security standards are implemented in my organisation (ex. ISO 27001 and ISO 27002).					
	6	International Cloud security standards are implemented in my organisation (ex. ISO 27017 and Cobit Cloud).					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Security and Privacy	7	Information Security standards are formalised and followed in my organisation.					
	8	Privacy is given high priority in my organisation.					
	9	Privacy is managed effectively in my organisation.					
	10	Information privacy training is provided for employees in my organisation.					
	11	International privacy standards are implemented in my organisation (ex. ISO/IEC 27018).					
Reliability	12	Information system reliability is given priority in my organisation.					
	13	I can count on information systems being continuously available in my organisation.					
	14	Unreliable information systems are immediately repaired or changed in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Reliability	15	Maximum acceptable downtime limits are set for each system in my organisation.					
	16	Precaution measures are put in place to avoid information system downtime in my organisation.					
Leadership	17	Top management supports information system project managers in my organisation.					
	18	Qualified project managers are assigned to information system projects in my organisation.					
	19	In the past, project managers contributed to the success of information system projects in my organisation.					
Project Planning	20	Information system project planning is a priority in my organisation.					
	21	A specific project team is assigned to information system in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Project Planning	22	Project plans are effective for the success of information system projects in my organisation.					
	23	Project plans are approved by top management in my organisation.					
	24	Information system project plans are based on international standards in my organization (ex. PRINCE2/PMP).					
Clear Requirements	25	Requirements gathering is an important stage for information system projects in my organisation.					
	26	A formalised process is followed for gathering information system requirements in my organisation.					
	27	Information system project requirements are clear in my organisation.					
	28	Information system requirement gathering is done effectively in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Top Management Support	29	Top management support information system projects in my organisation.					
	30	Top management provides information system projects with necessary resources in my organisation.					
	31	Top management continuously monitors information system projects throughout their lifecycle in my organisation.					
	32	Top management rewards/ penalizes teams working on successful/ failed information system projects in my organisation.					
	33	Top management in my organisation understands the benefits of migrating to the cloud.					
Policy and Legislation	34	Existing local government legislation and policies are effective.					
	35	My organization has the competencies necessary to comply with local policies and legislations.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Consultant Competency	36	External information system consultants are given support in my organisation.					
	37	There is a formal process for hiring external information system consultants in my organisation.					
	38	Previous external information system consultants have been competent.					
	39	External information system consultants follow a formal consulting process in my organization.					
	40	External information system consultants are hired based on competency in our organization (i.e. not based on lowest cost).					
Cooperation Coordination	41	Cooperation is encouraged between all information system stakeholders in my organisation.					
	42	Cooperation between information system project stakeholders is formalized in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Cooperation Coordination	43	On past information system projects in our organisation, cooperation between stakeholders was successful.					
	44	Coordination of legacy systems with new information systems is supported in my organisation.					
	45	Coordination of partner organisation's systems with new information systems is supported in my organisation.					
	46	Personnel are dedicated to oversee coordination of information systems in my organisation.					
	47	In the past, coordination of information systems has been successful in my organisation.					
Business Process Re-engineering (BPR)	48	Information systems are adapted to fit new business processes in my organisation.					
	49	BPR strategies are formalised and followed in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Business Process Re-engineering (BPR)	50	Systems are adapted successfully to fit new business processes in my organisation.					
	51	Training is provided for resources when new business processes are introduced in my organisation.					
	52	BPR is aligned with existing processes in my organization.					
Communication	53	A formal communication plan is followed in my organisation.					
	54	Communication plans are updated in my organization.					
	55	In the past communication has been effective on information system projects in my organisation.					
Standards	56	Information exchange follows international standards in my organisation.					
	57	A formal repository for information exchange is available in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Standards	58	The exchange of information is effective in my organisation.					
Training	59	Training for new information systems is given priority in my organisation.					
	60	Training improves the level of users' understanding of new information systems in my organisation.					
	61	Training gives users' confidence in using new information systems in my organisation.					
	62	Training sessions are taught by qualified professionals in my organisation.					
	63	Training materials are updated in my organisation.					
	64	Help desks are available to provide post –training support in my organisation.					
Knowledge Management	65	Formal techniques and strategies are used for sharing knowledge in my organisation.					
	66	Technology is utilised for sharing knowledge in my organisation.					

Factor	No	How often are these statements true about your organization?	Always	often	Some-times	Rarely	Never
Knowledge Management	67	Knowledge sharing is monitored in my organisation.					
Business Continuity	68	A Business Continuity and Disaster Recovery plan exists in my organisation.					
	69	Relevant staff are trained to activate the Business Continuity and Disaster Recovery plan in my organisation.					
	70	Business Continuity and Disaster Recovery plans are based on international standards in my organization (ex ISO 22301).					
	71	Existing Business Continuity and Disaster Recovery plans are sufficient to ensure business continuity in my organization.					

Bibliography

Abouzahra, M. (2011). Causes of failure in Healthcare IT projects. *3rd International Conference on Advanced Management Science* (pp. 46-50). Singapore: IACSIT Press.

Aharthi, A., Alassafi, M., Alzahrani, A., Walters, R., & Wills, G. (2017). Critical Success Factors for Cloud Migration in Higher Education Institutions: A conceptual Framework. *International Journal of Intellighent Computing Research*, 817-825.

AlAjmi, K. (2011). Is Cloud Computing Appropriate for Government? *International Conference on E-Learning, E-Business, Enterprise Information Systems, & E-Government* , (pp. 169-175).

Alassafi, M., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics*, 996-1010.

Alassim, M., Alfayad, M., & Abbott-Halpin, E. (2017). Understanding Factors Influencing E-Government Implementation in Saudi Arabia from an Organizational Perspective. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, 917 - 922.

ALdayel, A. I., Aldayel, M. S., & Al-Mudimigh, A. S. (2011). The Critical Success Factors of ERP implementation in Higher Education in Saudi Arabia: A case study. *Journal of Information Technology and Economic Development* , 1-16.

Aldraehim, M., Edwards, S. L., & Watson, J. (2012). Cultural impact on e-service use in saudi arabia: Results from focus groups . *Information Technology: New Generations (ITNG).* IEEE.

Alfaadel, F., Alawairdhi, M., & Al-Zyoud, M. (2012). Success and Failure of IT Projects: A Study in Saudi Arabia. *ACACOS proceedings of the 11th WSEAS international conference on Applied Computer and Applied Computational Science*, (pp. 77-82).

Bibliography

Alfarraj, O., Alhussain, T., & Abugabah, A. (2013). Identifying the Factors Influencing the Development of eGovernment in Saudi Arabia: The Employment of Grounded Theory Techniques. *International Journal of Information and Education Technology*.

Alfayad, M., & Abbott-Halpin, E. (2017). Understanding the current situation of E-Government in Saudi Arabia: A model for implementation and sustainability. *Proceedings of 17th European Conference on Digital Government, ECDG 2017*, (pp. 306–314).

Alghamdi, I., Goodwin, R., & Rampersad, G. (2014). Organizational E-Government Readiness: An Investigation in Saudi Arabia. *International Journal of Business and Management, 9*(5), 14.

ALHAMMADI, A. S. (2015). The Determinants of Cloud Computing Adoption in Saudi Arabia. *2nd International Conference on Computer Science and Engineering*, (pp. 55-67). Dubai.

Alharbi, F., Atkins, A., & Stanier, C. (2017). Holistic Sratigic Assesment and Evaluation of Cloud Computing Adoption: Insight from Saudi Healthcare Organisations. *Internet Technologies and Applications*. Wrexham: IEEE.

AlMajed, A. I., & Mayhew, P. (2013). CHIEF INFORMATION OFFICERS' PERCEPTIONS OF IT PROJECT SUCCESS FACTORS IN SAUDI ARABIAN PUBLIC ORGANIZATIONS: AN EXPLORATORY STUDY. *International Journal on Computer Science and Information Systems*, 66-78.

Almajed, A. I., & Mayhew, P. (2014). An Empirical Investigation of IT Project Success in Developing Countries. *Science and Information Conference*, (pp. 984-990). London.

Al-Mudimigh, A. S., Ullah, Z., & Alsubaie, T. (2011). A framework for portal implementation: A case for Saudi organizations. *International Journal of Information Management*, 38-43.

Al-Nuaim, H. A. (2011). An Evaluation Framework for Saudi E-Government. *Journal of e-Government Studies and Best Practices, 2011*, 1-12.

Al-Ruithe, M., Benkhelifa, A., & Hameed, K. (2017). Current State of Cloud Computing Adoption- An Empirical Study in Major Public Sector

Organizations in KSA. *Conference on Future Networks and Communications* (pp. 378-385). Elsevier B.V.

Alsanea, M. (2015). Factors Affecting the Adoption of Cloud Computing in Saudi Arabia's Government Sector. *Doctoral Thesis*. Goldsmiths University of London.

Alshehri, M., Drew, S., & Alfarraj, O. (2012). A Comprehensive Analysis of E-government services adoption in Saudi Arabia: Obstacles and Challenges. *International Journal of Advanced Computer Science and Applications, 3*(2), 1-6.

Alshomrani, S., & Qamar, S. (2013). Cloud Based E-Government: Benefits and Challenges. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING*, 15-19.

Al-Turki, U. M. (2011). An exploratory study of ERP implementation in Saudi Arabia. *Production Planning & Control*, 403-413.

Anastasi, A., & Urbina, S. (1997). *Psychological Testing.* Upper Saddle River: Prentice-Hall.

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*, 50-58.

Banerjee, A., Chitnis, U., Jadhav, S, Bhawalkar, J., & Chaudhury, S. (2009). Hypothesis testing, type I and type II errors. *Industrial Psychiatry Journal, 18*(2), 127-131.

Bartlett, J., Kotrlik, J., & Higgins, C. (2001). Organizational Research: Determining Appropriate sample Size in Survey Research. *Information Technology, Learning, and Performance Journal*, 43-50.

Berg, M. (2001). Implementing information systems in health care organizations: myths and challenges . *International journal of medical informatics*, 143-156.

Bibliography

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. Tampa: Global Text Project.

Bhisikar, A. (2011). G-Cloud: New Paradigm Shift for Online Public Services. *International Journal of Computer Applications* .

Boynton, A. C., & Zmud, R. W. (1984). An assessment of critical success factors. *Sloan management review*, 17-27.

Bullen, C. V., & Rockart, J. F. (1981). *A primer on critical success factors.* MIT.

Buller, A. (2016). *Saudi Arabia could warm to cloud computing, so long as regulation and connectivity keep pace.* Retrieved from computerweekly: http://www.computerweekly.com/

Buyya, R., Garg, S. K., & Calheiros, R. N. (2011). SLA-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions. *Cloud and Service Computing (CSC).* IEEE.

Cellary, W., & Strykowski, S. (2009). E-Government Based on Cloud Computing and Service-Oriented Architecture. *3rd international conference on Theory and practice of electronic governance.* ACM.

Chanchary, F. H., & Islam, S. (2011). E-government based on cloud computing with rational inference agent. *High Capacity Optical Networks and Enabling Technologies (HONET)* (pp. 261-266). IEEE.

Chen, X., Wills, G., Gilbert, L., & Bacigalupo, D. (2010). *Using Cloud for Reaserch: A TechnicalReview.* JISC Final Report.

Chen, Y. N., Chen, H. M., Huang, W., & Ching, R. K. (2006). E-government strategies in developed and developing countries: An implementation framework and case study. *Journal of Global Information Management*, 23.

CITC. (2016). *Saudi Arabia's telecom regulator proposes regulating cloud computing.* Retrieved from Communications and Information Technology Commission (CITC): http://www.citc.gov.sa/en/mediacenter/pressreleases/Pages/20160724001.aspx

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2 ed.). New Jersy: Lawrence Earlbaum Associates.

Creswell, J. W. (2013). *Qualitative Inquiry and Research: Choosing Among Five Approaches. .* Los Angeles: SAGE.

Cronbach, L. (1971). Test Validation. In R. Thorndike, *Educational Measurement* (pp. 443-507). D.C: American Council on Education.

Dada, D. (2006). .The Failure of E-Government in Developing Countries: A Literature Review. *The Electronic Journal of Information Systems in Developing Countries*, 1-10.

Davis, D. (1996). *Business Research for Decision Making.* Belmont: Duxbury Press.

De Vaus, D. A. (2002). *Surveys in Social Research.* NSW: Psychology Press.

DeVellis, R. (2012). *Scale development: Theory and applications.* Los Angeles: Sage.

Diez, O., & SIlva, A. (2013, March 13). Govcloud: Using Cloud Computing in Public Organizations. *IEEE Technology and Society Magazine*, pp. 66-72.

Dyba, T. (2000). An Instrument for Measuring the Key Factors of Success in Software Process Improvement. *Empirical Software Engineering*, 357-390.

El Sawah, S., Abd El Fattah Tharwat, A., & Hassan Rasmy, M. (2008). A quantitative model to predict the Egyptian ERP implementation success index. *Business Process Management Journal*, 288-306.

Elliot, D., Swartz, E., & Herbane, B. (1999). Just waiting for the next big bang: business continuity planning in the UK finance sector. *Journal of Applied Management Studies*, 43-60.

European Commission . (2010, January 26). *The Future of Cloud Computing.* Retrieved 8 2013, from CORDI: http://cordis.europa.eu/fp7/ict/ssai/docs/executivesummary-forweb_en.pdf

Bibliography

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior research methods*, 1149-1160.

Forster, N. S., & Rockart, J. F. (1989). *Critical success factors: an annotated bibliography.* MIT.

Franke, R., & Eckhardt, A. (2014). Crucial Factors for E Government Implementation Success and Failure: Case Study Evidence from Saudi Arabia. *Twentieth Americas Conference on Information Systems.* Savannah.

Ganesh, L., & Mehta, A. (2010). Critical success factors for successful enterprise resource planning implementation at Indian SMEs. *International Journal of Business, Management and Social Sciences*, 65-78.

Garrison, G., Kim, S., & Wakefield, R. L. (2012, September 9). Success factors for deploying cloud computing. *Communications of the ACM*, pp. 62-68.

GCCEGOV. (2013). *eGovernment Programs*. Retrieved December 2013, from Cooperation Council for the Arab States of the Gulf: http://gccegov.com/web/guest/egovernment-awareness

Géczy, P., Izumi, N., & Hasida, K. (2012). CLOUDSOURCING: MANAGING CLOUD ADOPTION. *Global Journal of Business Research (GJBR)*.

Girard, J. P., & Girard, J. L. (2015). Defining knowledge management: Toward an applied compendium. *Online Journal of Applied Knowledge Management*, 1-20.

Gliem, J., & Gliem, R. (2003). Calculating, Interpreting, And Reporting Cronbach's Alpha Reliability Coefficient For Likert-Type Scales. *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.* Ohio.

Gov, S. (2012). *The e-Government Second Action Plan.* Riyadh: Saudi Government.

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?An Experiment with Data Saturation and Variability. *Field Methods, 18*(1), 59–82.

Hodgkinson, S. (2012). *Why government agencies need the cloud.* OVUM.

Iglesias, R., Nicholls, R., & Travis, A. (2012). Private Clouds with No Silver Lining: Legal Risk in Private Cloud Services. *Communications & Strategies*, 125-40.

Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). *Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing.* First Monday.

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing.* NIST special publication.

Janssen, M., & Joha, A. (2011). CHALLENGES FOR ADOPTING CLOUD-BASED SOFTWARE AS A SERVICE (SAAS) IN THE PUBLIC SECTOR. *ECIS 2011 Proceedings.*

Jick, T. D. (1979). Mixing qualitative and quantitative methods: Triangulation in action. *Administrative science quarterly*, 602-611.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational researcher*, 14-26.

Jupp, V. (2006). *The SAGE Dictionary of Social Research.* SAGE Publications.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. . *MIS quarterly*, 571-586.

Karunanithi, D., & Kiruthika, B. (2011). Efficient Framework for Ensuring the Effectiveness of Information Security in Cloud Computing. *International Conference on Signal, Image Processing and Applications.* IACSIT Press.

Khan, F., Zhang, B., Khan, S., & Chen, S. (2011). Technological leap frogging e-government through cloud computing. *IEEE* , (pp. 201–206). Shenzhen.

Bibliography

Khandelwal, V. K., & Ferguson, J. R. (1999). Critical success factors (CSFs) and the growth of IT in selected geographic regions. *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences.* Maui: IEEE.

King, N., & Horrocks, C. (2010). *Interviews in qualitative research.* Sage.

Kooshesh, R., Mollahasani, M., & Barzegar, H. R. (2013). Implement E-Government Based Approach on Cloud computing. *Journal of Basic and Applied Scientific Research*, 488-493.

Krosnick, J. A., & Fabrigar, L. R. (1997). Designing Rating Scales for Effective Measurement in Survey. In *Survey Measurement and Process Quality* (pp. 141-163). New York: John Wiley and Sons.

Kundra, V. (2011). *FEDERAL CLOUD COMPUTING STRATEGY.*

Kurdi, R., Taleb-Bendiab, A., Randles, M., & Taylor, M. (2011). E-Government Information Systems and Cloud Computing (Readiness and Analysis). *Developments in E-systems Engineering (DeSE* (pp. 404-409). IEEE.

Lakshminarayanan, R., Kumar, B., & Raju, M. (2013). Cloud computing benefits for educational institutions. *Second International Conference of the Omani Society for Educational Technology.* Oman.

Liang, J. (2012). Government cloud: enhancing efficiency of e-government and providing better public services. *International joint conference on Service sciences (IJCSS).* IEEE.

Liang, J. (2012). Government cloud: enhancing efficiency of e-government and providing better public services. Shanghai: IEEE.

Likert, R., & Roslow, S. (1934). *The Effects Upon the Reliability of Attitude Scales of Using Three, Five or Seven.* New York: New York University.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing.* NIST.

Motwani, J., Mirchandani, D., Madan, M., & Gunasekaran, A. (2002). Successful implementation of ERP projects: evidence from two case studies. *International Journal of Production Economics*, 83-96.

Mreea, M., Munasinghe, K., & Sharma, D. (2016). A Stratigic Decision Value Model for Cloud Computing in Saudi Arabia's Public Sector. *International Conference on Computer and Information Sciences.* Okayama: IEEE.

Ndou, V. (2004). E – Government for Developing Countries: Opportunities and Challenges. *The Electronic Journal on Information Systems in Developing Countries*, 1-24.

Orakwue, E. (2010). Private Clouds: Secure Managed Services. *Information Security Journal*, 295-298.

Poon, P., & Wagner, C. (2001). Critical success factors revisited: success and failure cases of information systems for senior executives. *Decision support systems*, 393-418.

Preece, J., Rogers, Y., & Sharp, H. (2002). *Interaction Design. Beyond Human-Computer Interaction.* Somerset: John Wiley & Sons.

Rajan, R. A., & Shanmugapriyaa, S. (2012). Evoloution of Cloud Storage as Cloud Computing Infrastructur Service. *Journal of Computer Engineering*, 38-45.

Recker, J. (2013). *Scientific Research in Information Systems.* Berlin: Springer.

Riad, A. M., El-Bakry, & Hazem M, E.-A. G. (2010). A Novel DSS Framework for E-government . *International Journal of Computer Science Issues (IJCSI)*.

Rittinghouse, J. W., & Ransome, J. F. (2009). *Cloud computing: implementation, management, and security.* CRC press.

Rockart, J. F. (1979). Chief executives define their own data needs. *Harvard business review*, 81-93.

Saleh, M. F., Abbad, M., & Al-Shehri, M. (2013). ERP Implementation Success Factors in Saudi Arabia. *International Journal of Computer Science and Security (IJCSS)*.

Schouten, E. (2013). *IBM SmartCloud Essentials.* Packt Publishing.

Bibliography

Schuppan, T. (2009). Reassessing outsourcing in ICT-enabled public management. *Public Management Review*, 811-831.

Smith, D. M. (2017). *Gartner Insights on How and Why Leaders Must Implement Cloud Computing .* Retrieved from Gartner: https://www.gartner.com/imagesrv/books/cloud/cloud_strategy_leadership.pdf

Song, S.-h., Shin, S. Y., & Kim, J.-y. (2013). A study on method deploying efficient cloud service framework in the public sector. PyeongChang : IEEE.

Spector, P. (1992). *Summated Rating Scale Construction: An Introduction.* Newbury Park: Sage.

Tripathi, A., & Parihar, B. (2011). E-Governance challenges and cloud benefits. *IEEE.* Shanghai.

UN. (2014). *E-Government for the Future We Want.* New York: United Nations.

Vijaykumar, N. (2011). *Role of ICT in e-Governance: Impact of Cloud Computing in Driving New Initiatives.* Infosys Technologies Limited.

Walden, E., & Browne, G. (2002). Information cascades in the adoption of new technology . *ICIS* (p. 40). ICIS 2002 Proceedings.

Weber, A. S. (2011). Cloud computing in education in the Middle East and North Africa (MENA) region: Can barriers be overcome? *eLearning and Software for Education(eLSE) Journa*, 1.

West, D. M. (2010). *Saving money through cloud computing.* Governance Studies at Brookings.

Wyld, D. C. (2009). *Moving to the cloud: An introduction to cloud computing in government.* IBM Center for the Business of Government.

Wyld, D. C. (2010). THE cloudy future of government IT: Cloud computing and the public sector around the world. *International Journal of Web & Semantic Technology*, 1-20.

Yeh, C., Zhou, Y., Yu, H., & Wang, H. (2010). Analysis of E-government service platform based on cloud computing. *Information Science and Engineering (ICISE)* (pp. 997-1000). IEEE.

Yesser. (2011). *Yesser Anual Report.* Ryiadh: Government of Saudi Arabia.

Yesser. (2014). *Yessser Anual Report.* Ryiadh: Saudi Government.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, 7-18.

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud Computing in E-Government across Europe. *Springer .* Berlin Heidelberg.