Towards a framework for the successful implementation of a government cloud in Saudi Arabia

Amal Alkhlewi*, Robert Walters and Gary Wills

Cyber Physical Systems,

School of Electronics and Computer Science, University of Southampton, England

Email: aa3d12@soton.ac.uk Email: rjw1@ecs.soton.ac.uk Email: gbw@ecs.soton.ac.uk

Abstract: 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 standardising 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 critical 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 and confirmed by a methodological triangulation.

Keywords: cloud computing, government cloud, e-government, CSF; Saudi Arabia.

1 Introduction

The function of e-government is to provide efficient government management of and access to information for citizens, thus enhancing service delivery (UN, 2014). In 2005, Saudi Arabia commenced its e-government initiative called 'Yesser'. According to the Saudi e-government Program's website, the role of Yesser is 'enabling the implementation of e government' (Yesser, 2017). 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, 2011, 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' (Yesser, 2017). 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 and Eckhardt, 2014). When reporting on the first action plan in 2011, the weak ICT infrastructure in government organisations was emphasised 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 and Abbott-Halpin, 2017). In their 2014 study of Yesser et al. 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 organisations, citing weakness in the public sectors infrastructure as a justification for the change.

One proposed contributing factor 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 organisations 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).

Having a reliable technical infrastructure is a precursor for Yesser to succeed (Alfayad and 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 and Parihar, 2011; Zwattendorfer et al., 2013). It allows governments to uniformly supply e-government services, irrespective of the different maturity levels in different government agencies (Tripathi and Parihar, 2011). Many countries have begun to recognise the benefits of utilising cloud computing in government (Hodgkinson, 2012). In Europe, the leading utilisation 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). One factor shown to improve the effectiveness of government clouds is they must be established in their own countries (Yeh et al., 2010). Thus, 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.

1.1 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, 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 following sections, a literature review to identify the critical success factors for implementing a government cloud in Saudi Arabia is described.

1.1.1 *Cloud computing in the Saudi public sector*

In their study on 'The determinants of cloud computing adoption in Saudi Arabia', Ihammadi (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 organisations 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 organisations 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. For example, 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 CSFs to prepare for cloud implementation will 'mean greater probability of cloud success, with the organisation 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.

1.2 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 1. 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 and 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 and Qamar, 2013). Cloud computing security concerns the 'confidentiality, availability and integrity of data or information' (Karunanithi and Kiruthika, 2011). Jansen and 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 and 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 provider (Jaeger et al., 2009; Armbrust et al., 2010; Jansen and Grance, 2011). Janssen and 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) proposed the development of cloud computing regulations in the country (CITC, 2016). These regulations were published in 2018.

- **Other factors**

Uncoordinated adoption and lack of appropriate organisational and governance mechanisms in place could undercut the benefits of SaaS (Janssen and 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.

1.3 Challenges to IT projects in Saudi Arabia

Several success factors to implementing 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 organisational culture, proper project planning, clear vision and objectives, clear statement of requirements and lack of top management support. Almajed and 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 and Mayhew (2014) surveyed 72 CIO's in Saudi public organisations 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 organisations, 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 et al. (2013) Survey 74 employees from mostly government or joint government-private owned organisations to determine the factors critical to the success of ERP implementation in Saudi Arabia and conclude vendor support, consultant competence, business process re-engineering (BPR), 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 factors related to success and failure of Healthcare Information Systems projects in Saudi Arabia and identified the main causes of failure as being unclear scope, failure to identify and analyse risks associated with data integration, incompatibility with existing systems and data inconsistency and 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 organisations to identify CSF's and recognises good communication, user acceptance, top management support, clear goals and objectives and project monitoring and controlling as critical factors.

2 Framework for the successful implementation of a government cloud in Saudi Arabia

The framework for the successful implementation of a government cloud in Saudi Arabia was constructed in three stages. First, the success factors for the implementation of a government cloud were determined from the literature review. Following that, the success factors for implementing large scale IT projects in Saudi Arabia such as a private cloud, were identified. Finally, the factors identified in stages one and two were synthesised to form the framework for the successful implementation of a government cloud in Saudi Arabia. The framework is comprised of ten factors (see Figure 1). These components cover technical, organisational and management aspects and are described in the following sections.

- 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 government cloud, both technical coordination and organisational 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 government cloud. Leadership is required to explain, insure buy in and test the success of the project.

Figure 1 Proposed FSIGC

- Business process re-engineering (BPR)

To benefit completely from a private G-cloud, BPR 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 government 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 government cloud, top management support is essential. This support will ensure that the necessary resources and funds are provided.

- Consultant competence

To ensure the successful implementation of a government cloud in Saudi Arabia, the IT consultants and staff need to have the proper training and skills.

3 Evaluation of framework

This preliminary study applied a mixed method approach to evaluate the framework presented above. The mixed method approach was chosen to strengthen the results of the study by validating the findings through triangulation (Kaplan and Duchon, 1988). In the next section a description is given of how the triangulation was performed and of the individual methods applied.

3.1 Research methods

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 2. The results from each stage were then compared.

Figure 2 Triangulation validation method

First, data was collected from secondary research by reviewing related literature to build the proposed framework. 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 3).

Figure 3 Research methodology

3.2 Expert review

Interviews were used to conduct an exploratory study – as there was no previously developed 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 (Bhattacharjee, 2012).

3.2.1 Expert review sample size

Qualitative studies usually depend on non-probability sampling where participants are chosen based on non-random criteria (Bhattacharjee, 2012). In expert sampling, participants are chosen based on their knowledge in the area being studied (Bhattacharjee, 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.

3.2.2 Expert review process

The expert review was based on semi-structured interviews with twelve IT experts from Saudi government agencies. These experts were from different Saudi government and semi-government organisations in diverse 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-ended 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 objective of the open-ended questions was to identify further factors that had not been identified in the desk-based study.

The interview questions were pre-tested on two Saudi IT experts and two fellow researchers at the

University of Southampton. 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.

3.3 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 (Bhattacharjee, 2012).

3.3.1 Survey sample size

In qualitative research, random sampling is employed which allows the findings of the study to be generalised to the population (Bhattacharjee, 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 $(1 - \beta)$ 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. From this calculation it was determined that the minimum sample size is 15.

3.3.2 Survey design

This survey was performed by administering an online questionnaire to confirm the factors in the updated framework resulting from the expert review. Thirty IT experts from Saudi government agencies responded to the online survey. These experts were from different Saudi government and semi-government organisations in diverse locations around Saudi Arabia. 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. Thirty four participants completed the online survey but, four of those worked in the private sector and their responses were not relevant to this study.

The questionnaire is divided into two parts. The first part, asks three nominal questions about the respondents' organisation type and experience to confirm their eligibility for this study. The second part was constructed using a five point Likert-type scale (Bhattacharjee, 2012) with the following ratings: strongly agree = 1; agree = 2; neutral = 3; disagree = 4 and strongly disagree = 5. The purpose of the questions in this part is to confirm the proposed factors for the successful implementation of a private government cloud in Saudi Arabia. The 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.

3.3.3 Data analysis

As there are no previous studies on factors influencing the implementation of a 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 the following sections, the results from both the expert review and the survey are presented.

3.3.4 Results of expert review

Participating 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. The second question

was to identify factors not mentioned in the study. The remaining questions were used to identify challenges and barriers to the implementation of a private government cloud in Saudi Arabia. The experts' opinions were analysed and coded to produce the following results.

3.3.5 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 BPR 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'.

3.3.6 Additional factors

In question 2 of the interview, experts were asked 'What other factors do you recommend to ensure the successful implementation of a private G-cloud?' The purpose of this question is to identify factors not mentioned in the proposed framework. Answers are summarised as follows:

- training for the IT-team
- data knowledge and quality management
- business continuity plan
- disaster recovery plan
- communication
- standards and frameworks to govern the provided cloud services
- documentation
- standards for information exchange
- project management office
- transparency.
- Challenges
- Experts were asked to identify challenges to the implementation of cloud computing. The challenges identified are used to discover additional factors not mentioned in the proposed framework or determined in the previous section. The answers are summarised as follows:
 - We were expecting the product with the features with ease of use and self-service portal capabilities. But we are facing product limitations.
 - The most challenging task was the data centre facilities preparation.
 - Lack of local resources with cloud computing skills.
 - Lack of local training facilities.
 - Push from management to complete projects on unrealistic schedules.

- Security and privacy.
- Interoperability and portability.
- Reliability and availability.
- Legal aspects.
- Compatibility with existing systems.
- Training staff.

3.3.7 Results of survey

The questionnaire survey was conducted to confirm the factors identified from the expert review. The questionnaire was completed by thirty IT experts working in different Saudi government agencies. It consisted of close-ended questions. 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 organisation 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 organisations but have had previous experience of working in government organisations.

The purpose of the second part was to collect participants opinions on the factors revealed after the expertreview. 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'.

Table 1 Results of t test

<i>Factor</i>	<i>Mean</i>	<i>Sig. (2-tailed)</i>
Security	1.03	<.001
Privacy	1.13	<.001
Reliability	1.20	<.001
Policy and Legislation	1.67	<.001
Standards	1.30	<.001
Knowledge management	1.97	<.001
Cooperation	1.43	<.001
Coordination	1.40	<.001
Transparency	1.77	<.001
Sharing information	1.67	<.001
Business process re-engineering	1.80	<.001
Training for technical staff	1.40	<.001
Training for end-users	1.67	<.001
Top management support	1.20	<.001
Clear requirements	1.30	<.001
Proper planning	1.30	<.001
Project leader	1.30	<.001
Consultant competency	1.27	<.001
Business continuity	1.37	<.001
Disaster recovery	1.20	<.001

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 proposed factor is considered to affect the success of the implementation of a private G-cloud, if it has a mean value < 3 . Factors are considered to be statistically significant based on Bonferroni correction if the $p\text{-value} < 0.05 / (20) = 0.0025$. Table 1 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 $p\text{-values}$ are < 0.0025 .

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 and Gliem, 2003).

4 Discussions

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.

4.1 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 BPR. 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.

Figure 4 Confirmed framework

4.2 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 4.

these items. Following that, the goal will be developing a method for assessing the readiness of Saudi government agencies for the implementation of a private government cloud and setting guidelines for success.

5 Conclusions

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 was constructed based on reviewing relevant literature and synthesising the findings. The ten identified success factors are: security and privacy, reliability, cooperation and coordination, policy and legislation, leadership, BPR, project planning, clear requirements, top management support and consultant competence.

A mixed method triangulation methodology 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 are: communication, standards, knowledge management, training and business continuity.

Having identified 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

6 References

- Abouzahra, M. (2011) *Causes of Failure in Healthcare IT Projects*, pp.46–50, Singapore, IACSIT Press.
- Aharthi, A. et al. (2017) ‘Critical success factors for cloud migration in higher education institutions: a conceptual framework’, *International Journal of Intelligent Computing Research*, Vol. 8, No 1, pp.817–8
- AlAjmi, K. (2011). Is Cloud Computing Appropriate for Government? International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government. Las Vegas: World Congress in Computer Science, Computer Engineering, and Applied Computing., pp.169–175.
- Alassafi, M., Alharthi, A., Walters, R.J. and Wills, G.B. (2017) ‘A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies’, *Telematics and Informatics*, Vol. 31, No 5, pp.996–1010.
- Alassim, M., Alfayad, M. and Abbott-Halpin, E. (2017) ‘Understanding factors influencing e-government implementation in Saudi Arabia from an organizational perspective’, *International Journal of Information and Communication Engineering*, Vol. 11, No 7, pp.917–922.

Aldayel, A.I., Aldayel, M.S. and 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*, Vol. 2, No 2, pp.1–16.

Aldraehim, M., Edwards, S.L. and Watson, J. (2012) Cultural impact on e-service use in Saudi Arabia: results from focus groups In Latifi, Shahram (Ed.) Proceedings of the 2012 9th International Conference on Information Technology : New Generations, IEEE, Las Vegas,, pp. 744-750.

Alfaadel, F., Alawairdhi, M. and Al-Zyoud, M. (2012) Success and failure of IT projects: a study in Saudi Arabia, Proceedings of the 11th WSEAS international conference on Applied Computer and Applied Computational Science, Venice, Italy, pp.77–82.

Alfarraj, O., Alhussain, T. and Abugabah, A. (2013) 'Identifying the factors influencing the development of e-government in Saudi Arabia: the employment of grounded theory techniques', *International Journal of Information and Education Technology*, Vol. 3, No. 3, p.319.

Alfayad, M. and Abbott-Halpin, E. (2017) Understanding the current situation of e-government in Saudi Arabia: a model for implementation and sustainability. In: ECDG 2017 - Proceedings of the 17th European Conference on Digital Government. ACPI. Pp.306–314.

Alghamdi, I., Goodwin, R. and Rampersad, G. (2014) 'Organizational e-government readiness: an investigation in Saudi Arabia', *International Journal of Business and Management*, Vol. 9, No. 5, p.14.

Alhammadi, Stanier, Clare and Eardley, Alan. (2015) The determinants of cloud computing adoption in Saudi Arabia. In: 2nd International Conference on Computer Science and Engineering, Dubai, pp.28-29.

Alharbi, F., Atkins, A. and Stanier, C. (2017) *Holistic Strategic Assessment and Evaluation of Cloud Computing Adoption: Insight from Saudi Healthcare Organisations*, Wrexham, IEEE.

Almajed, A.I. and Mayhew, P. (2013) 'Chief information officers' perception of IT project success factors in Saudi Arabian public organisations: an exploratory study', *International Journal on Computer Science and Information Systems*, Vol. 8, No 1, pp.66–78.

Almajed, A.I. and Mayhew, P. (2014) An empirical investigation of IT project success in developing countries. In Proceedings of 2014 Science and Information Conference, London, pp.984–990.

Al-Nuaim, H.A. (2011) 'An evaluation framework for Saudi e-government', *Journal of e-Government Studies and Best Practices*, Vol. 2011, No 1, pp.1–12.

Al-Mudimigh, A., Ullah, Z., Alsubaie, T. (2011). 'A framework for portal implementation: A case for Saudi organizations', *International Journal of Information Management*, Vol.31, No 1, pp. 38–43. 10.1016/j.ijinfomgt.2010.05.001.

Al-Ruithe, M., Benkhelifa, A. and Hameed, K. (2017)' Current state of cloud computing adoption – an empirical study in major public sector organizations in KSA', *Procedia Computer Science*, Vol 110, No 1, pp.378–385.

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

Alshehri, M., Drew, S. and 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*, Vol. 3, No. 2, pp.1–6.

Alshomrani, S. and Qamar, S. (2013) 'Cloud based e-government: benefits and challenges', *International Journal of Multidisciplinary Sciences and Engineering*, Vol. 4, No 6, pp.15–19.

Al-Turki, U.M. (2011) 'An exploratory study of ERP implementation in Saudi Arabia',

Production Planning and Control, Vol. 22, No 4, pp.403–413.

Armbrust, M. et al. (2010) ‘A view of cloud computing’,

Communications of the ACM, Vol. 53, No. 4, pp.50–58.

Banerjee, A. et al. (2009) ‘Hypothesis testing, type I and type II errors’, *Industrial Psychiatry Journal*, Vol. 18, No. 2, pp.127–131.

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

Buller, A. (2016, April 26). Saudi Arabia could warm to cloud computing, so long as regulation and connectivity keep pace. Retrieved from computerweekly.com:

<https://www.computerweekly.com/news/450294175/Saudi-Arabia-could-warm-to-cloud-computing-so-long-as-regulation-and-connectivity-keep-pace> (accessed May 2019)

CITC. (2016, 7 24). Saudi Arabia’s Telecom Regulator Proposes Regulating Cloud Computing. Retrieved from citc.gov.sa: <https://citic.gov.sa/en/mediacenter/pressreleases/Pages/20160724001.aspx> (accessed May 2019)

Cohen, J. (1988) *Statistical Power Analysis for the Behavioral Sciences*, 2nd ed., Lawrence Earlbaum Associates, New Jersey.

Diez, O. and Silva, A. (2013) ‘Govcloud: using cloud computing in public organizations’, *IEEE Technology and Society Magazine*, 13 March, Vol. 32, No 1, pp.66–72.

Faul, F., Erdfelder, E., Buchner, A. and Lang, A.G. (2009) ‘Statistical power analyses using G* Power 3.1: tests for correlation and regression analyses’, *Behaviour Research Methods*, Vol. 41, No 4, pp.1149–1160.

Franke, R., & Eckhardt, A. (2014). Crucial Factors for E-Government Implementation Success and Failure. Twentieth Americas Conference on Information Systems. Savannah: AIS.

Garrison, G., Kim, S. and Wakefield, R.L. (2012) ‘Success factors for deploying cloud computing’, *Communications of the ACM*, 9 September, Vol. 55, No 9, pp.62–68.

Gliem, J. and Gliem, R. (2003) *Calculating, Interpreting and Reporting Cronbach’s Alpha Reliability Coefficient for Likert-Type Scales*, Ohio, s.n.

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

Guest, G., Bunce, A. and Johnson, L. (2006) ‘How many interviews are enough?’, *An Experiment with Data Saturation and Variability. Field Methods*, Vol. 18, No. 1, pp.59–82.

Hodgkinson, S. (2012) *Why Government Agencies Need The Cloud*, OVUM.

Iglesias, R., Nicholls, R. and Travis, A. (2012) ‘Private clouds with no silver lining: legal risk in private cloud services’, *Communications and Strategies*, Vol. 85, No 1, pp.125–40.

Jaeger, P.T., Lin, J., Grimes, J.M. and Simmons, S.N. (2009) *where is the cloud? Geography, Economics, Environment and Jurisdiction in Cloud Computing*, Vol. 14, No 5, First Monday.

Jansen, W. and Grance, T. (2011) *Guidelines on Security and Privacy in Public Cloud Computing*, s.l.: 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. Finland: AISel.

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

Kaplan, B. and Duchon, D. (1988) ‘Combining qualitative and quantitative methods in information systems research: a case study’, *MIS Quarterly*, Vol 12, No 4, pp.571–586.

Karunanithi, D. and Kiruthika, B. 2011, Efficient framework for ensuring the effectiveness of

information security in cloud computing, International Conference on Signal, Image Processing and Applications With workshop of ICEEA, pp. 1-10

Khan, F., Zhang, B., Khan, S. and Chen, S. (2011) Technological Leap Frogging e-Government through Cloud Computing, in Broadband Network and Multimedia Technology, IEEE.

Mreea, M., Munasinghe, K. and Sharma, D. (2016) A Strategic Decision Value Model for Cloud Computing in Saudi Arabia's Public Sector, in 15th International Conference on Computer and Information Science (ICIS) , Okayama: IEEE.

Orakwue, E. (2010) 'Private clouds: secure managed services',
Information Security Journal, Vol. 19, No 6, pp.295–298.

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

Saleh, M.F., Abbad, M. and Al-Shehri, M. (2013) 'ERP implementation success factors in Saudi Arabia', (*IJCSS*), Vol. 7, No 1, pp. 15-30.

Schuppan, T. (2009) 'e-government in developing countries: experiences from sub-Saharan Africa', *Government Information Quarterly*, Vol. 26, No. 1, pp.118–127.

Tripathi, A. and Parihar, B. (2011) *e-Governance Challenges and Cloud Benefits*, Shanghai, in International Conference on Computer Science and Automation Engineering, Shanghai: IEEE.

UK Cabinet Office (2011) *Government Cloud Strategy*. Retrieved from GOV.UK:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf (accessed September 2013).

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

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) Journal*, Vol. 2011, No 1, pp. 565-570.

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 and Semantic Technology*, Vol. 1, No 1, pp.1–20.

Yeh, C., Zhou, Y., Yu, H. and Wang, H. (2010) Analysis of e-government service platform based on cloud computing, Analysis of E-government service platform based on cloud computing. The 2nd International Conference on Information Science and Engineering (pp. 997-1000). Hangzhou: IEEE.

Yesser (2014) Annual Report 2014. Retrieved from Yesser E-Government Program:
https://www.yesser.gov.sa/EN/mediacenter/Annual_Reports/Annual%20Report%20for%20web.pdf. (accessed May 2019)

Yesser. (2011). Annual Reports 2011. Retrieved from Yesser E-Government Program:
https://www.yesser.gov.sa/EN/mediacenter/Annual_Reports/Annual_Report_for_web2011.pdf. (accessed May 2019)

Yesser. (2017, 10 30). The e-Government First Action Plan (2006 – 2010). Retrieved from Yesser E-Government Program:
https://www.yesser.gov.sa/en/MechanismsandRegulations/strategy/Pages/implementation_plan_first.aspx (accessed May 2019)

Zwattendorfer, B., Stranacher, K., Tauber, A. and Reichstädter, P. (2013) *Cloud Computing in e-Government across Europe*. Technology-Enabled Innovation for Democracy, Government and Governance, Berlin Heidelberg: Springer.