(IJRST) 2016, Vol. No. 6, Issue No. III, Jul-Sep e-ISSN: 2249-0604, p-ISSN: 2454-180X

# A RELATIONSHIP APPROACH TO INCREASING GOVERNMENT CONFIDENCE IN THE PUBLIC CLOUD FOR SENSITIVE DATA DEPLOYMENT

***Waleed Alghanim, **Feng Chen**

** PhD Candidate, School of Computer Science and Informatics, De Montfort University, UK*

***Senior Lecturer, Software Technology Research Laboratory, De Montfort University, UK*

## ABSTRACT

*Despite the numerous advantages of the public cloud governments are reluctant to deploy sensitive data in the public cloud because of lack of confidence about security. Governments are bound by legal and regulatory requirements and need a tailored public cloud solution that will offer them the level of governance they need over their data. Unfortunately, public cloud offerings are often standardised and providers do not offer governments what they need. The solution to this problem would be governments establishing a Service Level Agreement (SLA) through their relationship with the public cloud provider that gives government the confidence to place sensitive data in the public cloud. Towards a solution, this research examines the relationship between the government as a customer and the cloud provider in order to determine issues in the relationship that are contributing to this lack of confidence. The research is founded on theories and ideas about risk perception and tolerance, trust and collaboration for understanding the lack of confidence that governments have within the context of the relationship. Critical success factors of a successful government-cloud provider relationship are derived from the theories and used to inform the enquiry towards a new approach to the SLA relationship to increase government confidence in the public cloud.*

*Keywords—risk, trust, collaboration, government, public cloud, critical success factors*

## INTRODUCTION

The study is based on a premise that governments are not confident to migrate sensitive data and critical applications to the public cloud because of security and privacy concerns and that such concerns can be alleviated through an effective SLA or the relationship between the government and the cloud provider. The problem is that governments are not getting what they want in terms of security and privacy provisions and therefore may not be confident, this is due to the fact that because of the nature of the public cloud, services that are offered are often standardised.

Governments require a certain level of control over data and systems in order to be compliant with their laws and the only way that acceptable levels of governance can be achieved is through the SLA with the cloud provider. While this may seem easy to achieve governments are still

reluctant to use the public cloud for sensitive data. One solution to this problem is the development of technology that increases security and privacy in the cloud, the other solution is to increase government confidence in the public cloud through an improved SLA relationship.

The problem is that governments perceive a risk and this can affect their trust in cloud providers which also leads to a decline in collaboration. Therefore, this study considers theories and ideas about relationship risk perception, trust and collaboration towards improving the confidence of governments through improved SLA. The approach involves a number of critical success factors (CSFs) for an improved relationship that are derived from the theory. Additionally, critical success factors are derived from the frameworks, standards and ideas about the relationship between customers of the cloud and service providers in a procurement relationship, the frameworks and standards are designed to guide the customer, sometimes specifically governments, when considering a cloud provider and much of what is considered, such as governance which can be found in the SLA. Therefore, this study combines the CSFs derived from the two areas towards an approach where they are used to inform a study that examines the SLA relationship in order to understand the confidence issues where recommendations can be made.

## PRELIMINARIES

### A. *Security and privacy in the public cloud*

It is often recommended that sensitive data is not placed in the public cloud and that private clouds are more suitable due to the fact that government have less control over security and privacy in the public cloud (Bhatt , 2012, Khan et al. 2011). To provide an example, Lecklider (2014) says in reference to the US Department of Defense that some data is too sensitive for the public cloud. Diez and Silva (2013) say that careful consideration is needed when making decisions about whether services can be migrated to the cloud and that personally identifiable information is more at risk in the public cloud and therefore, requires anonymisation.

Government data includes highly sensitive data about citizens and the cloud as a storage solution for data is susceptible to hacking, even for data that is transmitted (Bhatt, 2012). Therefore, security is an important issue for governments and has to be considered on a number of different system levels which include the network itself which is located in the internet, applications or systems and data security (Zwattendorfer et al., 2013).

### B. *Governance*

Governance here refers to the level of control and oversight that governments have over their data and critical systems in the public cloud. Nycz and Polkowski (2015) say that governance is the main reason that causes concern in the public cloud because of the lack of physical control of the data. It is the nature of the public cloud that creates this governance issue because it is provided by a third party provider and hosted on a third party platform and which means that the

owner loses the ability to control the data. Moreover, the cloud is shared by multiple tenants and there also needs to be consideration of the employees of the cloud provider and service provider. Another issue related to the various parties is that they have their security agenda which may be in conflict (Almorsy, 2011).

Although the government owns the data, it is processed on an infrastructure that is owned by the cloud provider and the transitional nature of the cloud creates more loss of control over this data (Ahmad and Janczewski, 2011). This is not the case with private clouds where the physical infrastructure and data is controlled by government IT functions, there are no other parties to be concerned about and servers can be secured with their own firewall. However, with a public cloud most of this control is lost.

The European Union Agency for Network and Information Security (ENISA) Security & Resilience in Governmental Clouds also say it is already difficult for governments to manage their security in traditional IT environments and it is more difficult in the cloud because of the shift in balance of accountability for data operations, this is the case with the public cloud and the solution lies in an effective relationship between government and cloud provider (ENISA 2011).

Therefore, in order for governments to achieve the required governance in the public cloud there needs to be an effective relationship and negotiation with the cloud. Therefore, it is necessary to identify all of the areas in the relationship that are relevant to governance, these can be found in the frameworks and standards that govern that relationship and these can be used to inform the CSFs in the relationship that will lead to increased governance. An example of these areas includes the access rights of personnel from the third party cloud provider or data management policies.

### *C. Frameworks and standards for the cloud*

An improvement in the SLA relationship will lead to an increase in government's confidence to place sensitive data in the public cloud. This relationship is significantly informed by the frameworks and standards that governments use when considering the cloud. Specifically, these frameworks and standards offer guidelines to various aspects of the relationship and the SLA negotiation to ensure security in the cloud. While the CSfs may be derived from these frameworks and standards, they do not always consider the unique needs of government and sensitive data in the public cloud.

The Cloud Security Alliance (CSA) has presented a number of standards to guide those consider all cloud solutions and ensure security in the cloud. Particularly, CSA offerings focus on the relationship between customer and cloud provider. CSA has introduced Cloud Control Matrix (CCM) which is cross referenced with other standards and frameworks and is comprised of 16 domains which cover all areas that need to be considered in the SLA and include security,

continuity, governance and risk management, human resource security and transparency and accountability in the supply chain. One criticism of all the standards from CSA is that they apply to all types of organisation and all types of cloud solution and are not designed specifically for government in the public cloud, however, they do serve to inform about the different areas that need to be considered for a successful SLA relationship.

A standard that is used by the U.S. government is NIST, this standard offers a range of security and privacy controls for government information systems including the cloud. Although this standard is not designed for the cloud specifically, much of what it recommends is relevant. NIST places an emphasis on government in the public cloud and also considers protection from cyber-attacks and natural disasters and importantly offers guidance on non-negotiated and negotiated SLAs. This allows governments to negotiate data ownership, employee vetting, breach notification, the segregation and encryption of data, isolation of tenant applications, effectiveness reports and legal and regulatory compliance, all of these aspects will inform the CSFs for an effective SLA relationship.

ISO 27001 is widely used for information security management systems and their implementation. ISO 27001 is comprised of high level security objectives or control objectives. However, ISO focuses on the risks for an organisation and does not consider if an organisation is trustworthy enough to provide IT services, moreover, the scope of application of the certification is determined by the company, which may mean that not all offerings are certified (Almorsy et al, 2011).

In summary, partly the frameworks and standards are used to inform and govern the negotiated relationship between the government and the cloud provider as they inform governments what they need from that relationship. While there are criticisms of these frameworks and standards and they may in fact have limitations for governing these relationships, they do inform of the areas of the relationship that need to be considered and therefore, are useful for informing the CSFs.

## RISK, TRUST AND COLLABORATION

In the following a number of theories are presented which are related to risk perception, trust and collaboration as considered relevant to the relationship between the government as a customer and the provider of the public cloud. The theories are presented and their relevance to this relationship is explained.

### *D. Protection Motivation Theory (PMT)*

This theory is a common theory that is related to risk perception and risk tolerance. The theory says that people will protect themselves when they perceive a risk; they try to avoid negative consequences and feel that they have the ability to carry out preventative measures.

If PMT is applied to the government – cloud provider relationship if the risk perception is increased the use of protective action increases, such as not adopting the public cloud for sensitive data.

Moreover, one of the issues that governments have is that they need a certain level governance or control over the data not only for security purposes but also because it is required by legislation and regulation. The preventative measures in this case are the level of governance over the data in the cloud. Basically, the theory suggests that there is a relationship between risk perception and injury and that an organisation will take action if they are motivated and have the means (Campbell Institute, 2014), however, if they do not have the means, i.e. governance, then there will be higher risk perception. The way that this will inform the semi-structured interviews is that it will enquire about risk perception and how the government avoids it through governance.

### *E. Risk Compensation / Risk Homeostasis Theory*

Another theory that may provide an explanation about why governments are reluctant to place sensitive in the public cloud is Risk Compensation / Risk Homeostasis Theory. This theory basically states that a person will take more risk when there is greater security; risk taking behavior is directly related to the safety measures that are in place (Campbell Institute, 2014). If this theory is applied to the present study then it would suggest that the reason they are not taking the risk to place sensitive data in the public cloud is because there may be the perception that there are not enough security measures in place to protect sensitive data, after all the government are bound laws and regulations concerning citizen data. These security measures could include the level of governance, if the government has the security measures in place and the level of governance that they require then they would be willing to take more risk by placing sensitive data into the public cloud. This is related to the provisions that the service provider is willing to offer in the SLA, and will help to inform the enquiry into this relationship, specifically in relation to risk perception and risk tolerance.

### *F. Relationship risk and trust*

Service procurement, especially at the public level and especially in public cloud procurement where, for example, citizen data is concerned involves complex risks because the procurement process itself is complex. The present study is motivated by the fact that governments do not have the confidence to place sensitive in the public cloud because they are concerned about security risks. Therefore, it is important, within the theoretical framework to consider the issue of this risk perception within a public procurement relationship. In the literature about collaboration and partnership it can be found that there is a link between relationship risk and trust. These ideas are used to inform the study in terms of which aspects of the government / cloud provider relationship need to be investigated.

### *G. Collaboration fluency*

Research into collaboration and partnership in public service sector procurement has received much interest and has been studied from different perspectives including efficiency, effectiveness,

performance and success; however, according to Grudinschi et al. (2014) there have been few studies that specifically focus on procurement in public sector procurement.

Collaboration efficiency refers to the cost of collaboration which is not directly related to the aims and objectives of the present study. Collaboration effectiveness is about evaluating the ways that objectives are achieved from a managerial perspective (Grudinschi et al. 2014) which will be considered in the present study because objectives are identified by management using the frameworks, standards and models that guide procurement of the cloud for government services. Collaboration is a much broader concept and involves economic, operational and managerial indicators, the latter possible being relevant to the present study. Finally, there is concept of collaboration success which is related to satisfaction or dyadic sales (Grudinschi et al. 2014).

Collaboration is one of the important areas in order to provide high quality services and although collaboration practices and relationships have evolved in this area, there is still difficulty in gaining fluent collaboration between the partners (Grudinschi et al. 2014). More specifically, collaboration fluency is a newly defined concept, similar to collaboration effectiveness, and takes into account managerial indicators which include identifying common goals and challenges. In the case of the present study the common goal of the cloud service provide and the government as a customer would include security, planning to achieve the goal, implementing the plan and then analyzing and developing the activity (Grudinschi et al. 2014). Partnerships, in the case of the present study the partnership between the buyer and supplier, are related to the management of collaboration (Grudinschi et al. 2014).

Understanding the risks of the relationship gives a better understanding of risk management. There have been a number of different studies that have looked at risk management and the perception of risk related to collaboration management. The effect of trust on relationship risks in partnerships , how communication affects risk management and the effect of organizational structure on the perception of relationship risks are all examples of how different factors can have an effect on risk management and risk perception (Grudinschi et al. 2014). Unfortunately, according to Grudinschi et al. (2014 p.83) 'However, risk perception and relationship risk management are rarely highlighted in discussions of public procurement and collaboration'.

Blomqvist et al. (2008) examines the role of trust in contracts in companies that are technology intensive and puts forward three propositions about the role of trust and contracting in these types of companies. Firstly, trust is about what the other party will do in a situation that is often not included in the contract.In fact, formal contracts only play a limited role and have to be augmented by informal norms and agreements (Blomqvist et al., 2008). Much like the situation in the present study, when companies are engaged in this type of partnership they have to share valuable information and this information cannot always be covered by the contract, therefore, it requires trust. Moreover, similar to ideas put forward by Grudinschi et al. (2014) if the partners are able to

trust each other then it will lead to better communication and collaboration, and also enhances the transfer of information. A key consideration here is to what extent are governments allowed to trust cloud service providers given the laws and regulations that they must abide by.

Another point raised by Blomqvist et al. (2008) is that trust is a more important governance mechanism for companies dealing with technology than other companies. Moreover, that instead of being something that takes time to develop trust may be something that can develop quickly if there is an intense interaction of managers negotiating within a collaboration and may enable a collaborative relationship (Blomqvist (2005). In fact, as pointed out by Blomqvist (2005) with technology intensive partnerships fast-based trust was essential for partnership formation. Therefore, trust and collaboration are linked, but here it has been shown that trust is something that cannot necessarily be controlled by a contract. In reference to the present study, these ideas can inform the interviews through the development of questions related to trust, specifically, as mentioned in the above, the extent to which governments trust, and are allowed to trust service providers.

According to Thomson et al. (2009) there are five areas of collaboration that have emerged from the literature, these are governance, administration, organisational autonomy, mutuality and norms. Each of these is briefly presented below together with the relevance to the present study and how they contribute as CSFs which will in turn inform the inquiry into the relationship.

*1)* **Governance**

Decisions about the rules that will govern behavior and the relationship should be made jointly by both parties for there to be successful collaboration (Thomson et al. 2009). Specifically, this involves establishing a set of rules about who is authorised to make certain decisions, which actions are allowed and which are not and what information has to be provided. The governance here is very clear related to the governance that is referred to in the literature about government and cloud provider relationships where government require a certain level of governance in order to comply with their own laws and regulations. Having the authority to make certain decisions, establishing who is allowed to do what and rules about sharing information are found in the literature about cloud provider and customer relationships, especially under the area of governance.

Moreover, the process of governance is ongoing, there should be continuous negotiation to establish an equilibrium where although conflict may still occur marginally, there is still agreement on the rules for a collaborative environment achieved by managers understanding the agreed shared responsibility (Thomson et al. (2009).

*2)* **Administration**

An administrative structure is required to move from governance to action, here the focus is on implementation and management as opposed to governance where the focus is on institutional supply (Thomson et al. 2009). However, this implementation in collaboration is not easy to achieve because of the autonomous or semi-autonomous nature of the relationship whereby tradition mechanisms for coordination, such as hierarchy, do not work (Thomson et al. 2009).

An effective system for ensuring collaboration requires clarity of roles and responsibilities, mechanisms to measure each other's activities especially in terms of roles and responsibilities, and communication in order to enhance the coordination, these ideas will inform the Critical Success Factors (CSFs). However, these can be difficult when the communication is relational and not routinised (Thomson et al. 2009). One of the problems of collaboration is that the administrative structures are decentralised and there is a need for a central function for organising and distributing information, communication and reminding each partner about the rules that govern the partnership, again another CSF to consider in the relationship (Thomson et al. 2009).

*3)* **Organisational autonomy**

Partners have a dual identity, on the one hand they have their own identity and organisational authority, and on the other they have a collaborative identity. Therefore, there is a conflict between self-interests in wanting to achieve their own missions and maintaining an identity that is distinct from the collaboration and the collaborative interests which include achieving collaborative goals (Thomson et al. 2009). Problems arise from the fact that there is no formal authority hierarchy between the partners. This is an issue that can be considered in the inquiry as a CSF of a collaborative relationship.

*4)* **Mutuality**

Based on the idea of interdependence, mutuality means that each partner in the collaboration should enjoy mutual benefits according to their different interests or shared interests (Thomson et al. 2009). Mutuality occurs where one party has resources such as skills or expertise that the other party could benefit from, in reference to the present study, the government require the skills and expertise from the cloud provider, however, it is difficult to determine the benefits for the cloud provider apart from monetary reward and therefore, in reference to mutuality, it would be difficult to see why the cloud provider would give up their right to pursue their own interests at the expense of the government.

*5)* **Norms**

This is based on the idea of reciprocity, that in collaboration each party has a reciprocal obligation to each other and they expect that their contribution will be reciprocated by the partner (Thomson et al. 2009). In the case of the present study, because the government will pay the provider there will be the expectation that the cloud provider will reciprocate by providing the

services with the level of security that there government require. Clearly this idea is based on trust which is important in collaboration; unfortunately, this trust takes time and has to be built on a number of different interactions in order to build reputations (Thomson et al. 2009). The latter point will inform the inquiry of the present study where it is important to establish whether or not the government feels they have established this type of relationship that takes time, or that confidence is low because they have not had long enough to establish this type of relationship with the cloud provider.

## CRITICAL SUCCESS FACTORS

A study that investigates the relationship, especially during negotiation and formulation of the SLA, between governments and providers of the public cloud, towards understanding why governments are not confident to place sensitive data in the public cloud should consider theories and ideas about risk perception, trust and collaboration. CSFs will be based on these theories and ideas and used to inform the interviews with government officials to determine reasons for reluctance to move to the public cloud. However, as has been mentioned in the above, this relationship is also informed by frameworks and standards for cloud procurement and therefore, it is necessary to derive critical success factors from these as well. Therefore, this study offers a framework, based on CSFs derived from a combination of theories, ideas, frameworks and standards. In some cases link between the two are, for example, collaboration theory suggests establishing roles and responsibilities, an idea that is also found in cloud procurement frameworks.

### *H. Deriving CSFs from theory*

A number of CSFs relevant to the relationship being investigated are derived from risk, trust and collaboration theory, if they are achieved there will be an ideal relationship between the government and the cloud provider and according to the theory mentioned in the above a lower perception of risk, increased risk tolerance, increased trust and a better collaborative relationship. The CSFs will be derived from the theories found in the theoretical framework described in the above and ideas found in the literature and will form the basis for the development of inquiry with those government officials charged with the responsibility of cloud-related decisions.

In the study by Grudinschi et al. (2014) the CSFs include trust and communication. Other CSFs in the business relationship management and collaboration literature include the definition of common goals and objectives, the governance form of the operation, establishing roles and resources between partners, the norms of trust and mutuality, information sharing and communication mechanisms (Hoffman and Schlosser, 2001, Thomson et al. 2009).

As an example of a CSF, according to Koza and Lewin (2000) the success of a strategic alliance depends on the symmetry between their respective strategies. From the literature it is known that one of the problems for government is that cloud providers offer a standardised service because they depend on economies of scale and therefore, their strategic approach will not be aligned with

the government's strategic approach. This idea will inform the present study as a CSF and will inform questions about strategic symmetry between the government and the cloud provider.

### *I. Combining CSFs to inform enquiry*

Table 1 below illustrates where CSFs and sub CSFs derived from theories and frameworks are used to inform inquiry into the relationship.

In the examples that are provided in the table below (Table 1) the theory and the literature inform about the important areas that are required in the government – cloud provider relationship, within each area there are specific areas that are the CSFs for a successful relationship in terms of the government getting from the relationship what they want so that they have the confidence to place sensitive data in the public cloud. Each CSF has sub-critical success factors which need to be carried out in order to ensure that there is trust and collaboration in the relationship and a reduction in risk perception.

As an example, the governance form of the operation means that not only should there be clarity about governance but also the government would require a certain level of governance. As a CSF if the government is to achieve a certain level of governance, they need to, for example, establish authorisation for actions or decisions. These ideas will inform the inquiry, for example one of the critical success factors of a relationship is defining common goals, this is also one of the factors for collaboration effectiveness, therefore, when developing questions for any inquiry these CSFs will be considered, for example 'do you and your service provider share common goals?'

TABLE I. COMBINED CSFS FOR RELATIONSHIP INQUIRY

| | **Theory / Literature – Risk, Trust and collaboration**<br><br>**Government in the cloud – frameworks and standards** | **Critical Success Factor** | **Sub Critical Success Factor – theories and frameworks**<br><br>**Informs inquiry** |
|---|---|---|---|
| **RISK PERCEPTION TRUST COLLABORATION** | Governance | Require certain level of governance | Establishing authorization for actions or decisions<br><br>Establishing roles and responsibilities |

| | | | |
|---|---|---|---|
| | | | Establish rules about sharing information |
| | Administration | Effective system for ensuring collaboration | Clarity of roles and responsibilities<br><br>Mechanism for measuring other party's activities<br><br>Effective communication to enhance coordination of activities |

## CONCLUSION

Governments are reluctant to place sensitive data in the public cloud because they lack confidence in the cloud providers in terms of being afforded the required levels of security, privacy and governance over data. Governments will have more confidence if their needs are supported and if they have an effective relationship with the cloud provider. This was linked to theories and ideas about risk perception, trust and collaboration and ideas about what is required in a relationship between a government and a cloud provider derived from frameworks and standards, partly designed to govern this relationship. The approach to understanding the relationship concerns is based on the application of CSFs derived from the aforementioned theories and ideas and frameworks and standards, where common links were found between the two to establish CSFs that were applied to the inquiry into the relationship. Considering this relationship solely from the perspective of theories and ideas about risk, trust and collaboration would not provide as much in-depth insight into a relationship in this specific context. There is a need for consideration of what is required in a successful government – cloud provider relationship including the public cloud and sensitive data. For this it was therefore necessary to also derive CSFs from the frameworks and standards that inform this specific type of relationship.

## REFERENCES

[1] Ahmad, R Janczewski, L (2011). Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective. 2011 IEEE 4th International Conference on Cloud Computing. 372 - 381.

[2] M. Almorsy, J. Grundy, A. Ibrahim. (2011). Collaboration-Based Cloud Computing Security Management Framework. 2011 IEEE 4th International Conference on Cloud Computing, 364 - 371.

[3] D. Bhatt, (2012). A Revolution in Information Technology - Cloud Computing. Walailak Journal. 9 (2), 107 - 113.

[4] K. Blomqvist, P. Hurmelinna & R. Seppänen. 2005, "Playing the collaboration game right—balancing trust and contracting",*Technovation*, vol. 25, no. 5, pp. 497-504.

[5] K. Blomqvist, P. Hurmelinna-Laukkanen, N. Nummela, & S. Saarenketo. 2008, "The role of trust and contracts in the internationalization of technology-intensive Born Globals", *Journal of Engineering and Technology Management*, vol. 25, no. 1, pp. 123-135.

[6] Campbell Institute. (2014). Risk Perception; Theories, Strategies and Next Steps. National Safety Council, 1 - 11.

[7] O. Diez, A. Silva. "Govcloud: Using Cloud Computing in Public Organizations." Technology and Society Magazine, IEEE 32.1 (2013): 66-72.

[8] D. Grudinschi, S. Sintonen, & J. Hallikas. 2014, "Relationship risk perception and determinants of the collaboration fluency of buyer-supplier relationships in public service procurement",Journal of Purchasing and Supply Management, vol. 20, no. 2, pp. 82-91.

[9] W.H. Hoffmann & R. Schlosser, 2001, "Success Factors of Strategic Alliances in Small and Medium-sized Enterprises—An Empirical Survey", *Long Range Planning*, vol. 34, no. 3, pp. 357-381.

[10] F.Khan, B.Zhang, S.Khan, S.Chen. (2011). Technological Leap Frogging E-Government Through Cloud Computing.Proceedings of IEEE, 201 - 206.

[11] M. Koza & A. Lewin. 2000, "Managing partnerships and strategic alliances: raising the odds of success", European Management Journal, vol. 18, no. 2, pp. 146-151.

[12] T.Lecklider. (2014). Good enough for government work. Cloud Computing, 18 - 19.

[13] M. Nycz, Z. Polkowski. (2015). Cloud Computing In Government Units.2015 Fifth International Conference on Advanced Computing & Communication Technologies. 513 - 520.

[14] A. M. Thomson, J.L. Perry, & T.K. Miller. 2009;2007;, "Conceptualizing and Measuring Collaboration", Journal of Public Administration Research and Theory, vol. 19, no. 1, pp. 23-56.

[15] B. Zwattendorfer, K. Stranacher, A. Tauber, P. Reichstädter - "Cloud Computing in E-Government across Europe - A Comparison", Technology-Enabled Innovation for Democracy, Government and Governance Lecture Notes in Computer Science Volume 8061, 2013, pp. 181-195.