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

SUITABILITY OF FRAMEWORKS, STANDARDS AND CERTIFICATION FOR GOVERNMENT ADOPTION OF THE PUBLIC CLOUD FOR ADVANCED DIGITAL CONTINUITY

***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

There is increasing use of the public cloud by governments; however, this use is for non-critical systems and non-sensitive data. The potential that the public cloud has for government use lies not in the well-known benefits of cost and scalability, but also as a more permanent solution for providing e-services to citizens and as a solution for an advanced form of digital continuity whereby in the case of a national crisis, the government can continue to function in the public cloud on an indefinite basis. To take advantage of the public cloud in this way it becomes necessary for governments to place sensitive data and critical systems in the public cloud, which they are reluctant to do because of security concerns. Towards a solution to this issue, this study examines the frameworks, standards and certification schemes (FSCs) that inform governments' approach to adopting the public cloud. The study focuses on the extent to which they are suitable for the identification of issues related to the public cloud and its use for advanced digital continuity of government.

Keywords— government, public cloud, senstive data, digital continuity, cloud standards

INTRODUCTION

Governments often use private cloud solutions for e-government provision where the cloud infrastructure is located within their borders and although this offers a more secure solution than the public cloud, increasing confidence to deploy sensitive data and critical systems, governments cannot take advantage of the cost, scalability, portability and digital continuity benefits that are offered by the public cloud. Unfortunately, governments have been reluctant to deploy sensitive data to the public cloud because they are obligated by their own laws and international laws to provide a certain level of privacy and security over citizen data.

An additional benefit of the public cloud is that it can offer governments an advanced form of digital continuity. In the case of a disaster where the physical infrastructure of a private cloud solution could be destroyed, the public cloud could offer a digital continuity solution on an indefinite basis which would allow governments to continue to function by offering services to citizens. This idea is based on the project embarked upon by the government of Estonia and Microsoft, whereby they are seeking a digital continuity solution through the public cloud. Estonia is a country that is under threat from Russia both in terms of a physical incursion and a cyber-

attack, initially, the government developed a data embassy solution where it hosted private clouds in foreign embassies; however, this was still susceptible to attack so they developed a 'virtual data embassy' solution in the public cloud so that in the case of a disaster the country could continue to function in the public cloud, this was especially needed since Estonia is one of the most digitised countries in the world.

When governments consider a cloud solution they often refer to FSCs as part of their strategy to not only consider the solution but to guide them in the process of adoption. Unfortunately, these FSCs were not designed specifically for governments seeking a public cloud solution. There are special considerations in terms of security and privacy when considering the public cloud as a solution which the frameworks, standards do not fully address despite addressing security and privacy concerns of governments generally.

This study assesses the suitability of these frameworks, standards and certification schemes for the adoption of the public cloud by governments for an advanced digital continuity solution.

PRELIMINARIES

A. *E-government in the Cloud*

Governments are seeking to improve the public sector using cloud computing (Bhatt, 2012) because they are under increasing pressure in terms of budgets and the increasing demand services (Diez and Silva, 2013). Cloud technology does have numerous advantages for governments including cost savings and scalability; however, governments do face challenges which include issues related to implementation, security and privacy and if not managed properly could lead to a damaged reputation and a loss of public confidence (Aziz et al., 2013). Diez and Silva (2013) in examining the benefits and impacts of cloud computing, question why governments have not been as enthusiastic to use the cloud as other organisations. In Europe the most popular use of the cloud is G-cloud model which is a private or community cloud intended for use by the government (Zwattendorfer et al., 2013), however, this is not a public cloud solution.

B. *Security and Privacy Issues*

Although there are numerous advantages for e-government using the cloud, security and privacy concerns are often the main barriers to adoption (Luna et al., 2011, Bhatt, 2012). Governments have to be particularly concerned about these issues because of the need to protect sensitive citizen data and the cloud can be vulnerable for both data that is transmitted and stored (Bhatt, 2012). The cloud is a relatively new technology and there are concerns about security and privacy in different areas of cloud computing which include the cloud provider as the host, the network, data and applications (Hashizume et al., 2013, Zwattendorfer et al., 2013).

Such security concerns are related to risk factors such as use of the 'public' internet, multi-tenancy, data storage and lack of governance over data and systems in the cloud and traditional security measures such as authentication, authorisation and identity are not suitable for the cloud (Hashizume et al., 2013).

Moreover, although security controls in the cloud are the same for any other IT environment, due to cloud operational models and technology used in the cloud the risks are different (Hashizume et al., 2013).

C. *Sensitive and non-Sensitive Data*

A pertinent issue for governments considering use of the public cloud is whether to deploy sensitive or non-sensitive data. There have been recommends that sensitive data be deployed only in private clouds and that the public cloud should be used only for non-sensitive data (Bhatt, 2012, Khan et al., 2011). Citing an example of government agencies in the U.S., Lecklider (2014) suggests that some data is too sensitive to be placed on a commercial cloud. Diez and Silva (2013) suggest anonymising personally identifiable data before migration to the cloud and also suggests that careful consideration of services that can be moved to the cloud.

D. *Political and Legal Issues*

Governments have to comply with laws and regulations, domestic and international, that govern the data of it citizens, especially sensitive data. Governments need to consider the legal implications of the public cloud before the technical requirements (Diez and Silva, 2013). Examples of these legal implications include the case of the EU where public organisations are not allowed to transfer data outside of the EU because of the EU Data Protection Directive (Hashemi, 2013) and the US Patriot Act that allows data to be seized for investigation. In a public cloud solution legal issues arise due to the fact that data is held in different jurisdictions which may have their own laws, this may lead to loss of governance over data where the government of another country may have the right to subpoena data for investigation purposes. If geography and politics become fractured then the advantages of the public cloud solution can be undermined (Bhatt, 2012).

E. *Governance*

One of the main concerns for governments deploying to the public cloud is governance. Governance is the level of control that governments have over data and systems in the cloud and governance is lost because governments do not have physical control over the data in the public cloud (Nycz and Polkowski (2015). Therefore, there is a need for enhanced collaboration between the cloud provider and the government in order to increase governance (Rebollo et al., 2012).

F. *Digital Continuity (Advanced)*

In consideration of the need for digital continuity and disaster recovery, cloud computing should be considered as a first option (Scotland, 2014). Decmar and Vintar (2013) propose a solution for long-term digital continuity of e-government in the cloud using a centralised depository.

The government of Estonia has engaged in defensive moves to protect data integrity and security using private clouds held in friendly embassies around the world, however, they are still faced

with the threat of a physical incursion into its territory by Russia. Estonia's proposed solution is at the forefront of government in the public cloud and digital continuity and involves a solution where enough data and systems, both sensitive and non-sensitive, are placed in the public cloud so that the government can to continue to function in the cloud and provide services to citizens on an indefinite basis. This solution has required a whole new approach to considering the public cloud for government with considerations related to security and privacy beyond that offered by current frameworks and standards designed to guide governments in the cloud. This advanced form of digital continuity is a step beyond other governments who are only now embarking on the public cloud for normal services with restrictions on sensitive data.

ISSUES IN THE PUBLIC CLOUD

Because of the nature of the public cloud there are a number of issues that arise in relation to security, privacy and the use of the public cloud for digital continuity. These issues are mainly centred on the idea of governance in the cloud, specifically governance over the data and how it is managed.

G. *Governance*

Due to the nature of the public cloud in that it is hosted by a third party provider and hosted physically on a remote platform, there is a considerable loss of governance over the government's data. In reference to the parties that are involved, there is the cloud provider and the cloud service provider and in addition to this the cloud is shared by multiple tenancies, all of these create consideration for governance over government data in the public cloud. Although government owns the data, it is processed on a platform that is owned by the cloud provider.

H. *Security*

Specifically, in reference to security it is a service that is offered by the cloud provider which makes it difficult for the government to manage their security requirements because there is a shift in the balance of responsibility and accountability for governance and control over data (ENISA 2011). Similar areas of concern for security that are related to the nature of the public cloud include shared resources, third party hosting, multiple tenancies and multiple access points into the public cloud.

Each of the three parties, namely, the cloud customer, cloud service provider and cloud provider, that are involved in the relationship have their own approaches to security that may conflict (Almorsy, 2011). Although each party has their own Security Management Process that they wish to impose in the cloud, there is not one party who can control the security of the cloud services because no single party has a complete picture of all cloud processes (Almorsy, 2011).

FRAMEWORKS, STANDARDS AND CERTIFICATION SCHEMES (FSCS)

In considering government deployment of sensitive data to the public cloud there should also be consideration of the FSCs that governments use in making decisions about how and what can be

deployed. There are numerous frameworks, standards and certifications available that have been developed for cloud solutions other than the public cloud, or where the public cloud is considered, it is for private companies, however, the specific combination of government, the public cloud and sensitive data is not addressed by the FSCs. Although it should be noted that much of what is considered in these frameworks is still relevant and useful, however, this study is concerned with where they fall short for governments wishing to place sensitive data in the public cloud which may include the need for an advanced digital continuity solution.

I. *Criteria for Selection of FSCs*

Numerous FSCs are available for deployment to the cloud, however, these are far too numerous to consider and therefore, only those FSCs that consider security in the relationship between the cloud provider and customer, is intended for or can be used by the public sector and can be applicable to sensitive data in the public cloud are considered.

These criteria also inform the assessment criteria for the FSCs with the additional consideration of an advanced form of digital continuity whereby governments can continue to function in the public cloud on an indefinite basis in the case of a disaster.

J. *Identified FSCs for Sensitive Government Data in the Public Cloud*

FSCs were selected on the basis that they consider the transparency and governance that is required by governments in order to place sensitive data in the public cloud. The following frameworks consider, albeit to a certain extent, sensitive data as well as critical systems in the public cloud and are evaluated against these factors and their suitability for assisting governments for advanced digital continuity.

1. CSA Guidance
2. CSA Cloud Control Matrix
3. CSA Consensus Assessment (CAIQ)
4. ENISA Security Framework for Governmental Clouds
5. NIST (800-144)

1) CSA Guidance

The CSA (Cloud Security Alliance) Guidance does consider the public cloud as well as other types of cloud such as private clouds. In reference to governance which is the most important consideration for governments, the CSA guidance includes information security guidance, risk management and compliance, all of which are related to required levels of governance. The emphasis in the CSA Guidance in this regard is on the provision of information as part of achieving increased governance. For example, the guidance says that information security should be provided across the supply chain which includes providers, customers and third-party vendors. Moreover, towards achieving governance the guidance also emphasises the importance of the

relationship between customer and provider and where possible in a custom solution all details should be negotiated.

The guidance emphasises information management and governance which is relevant to governments and governance over data. Information governance here includes location and jurisdictional policies which is concerned with the legal implications of the geographic location of data, something that is important for governments placing sensitive data in the public cloud. Other areas related to information governance include authorisations which is about who can access what information, responsibility for ownership of the information and custodianship of information on behalf of the information owner all of which address the concerns of government in the public cloud.

In reference to Enterprise Risk Management (ERM) the guidance recognises that there are numerous variables that need to be considered if a cloud solution is to be adopted. The guidance recommends that cloud services and security should be addressed as supply chain security issues and includes assessment of the cloud provider's supply chain; this is relevant to governments because they have to abide by strict laws and regulations and are accountable for any risk to sensitive data, especially that of citizens, which means they have to assess all potential risks in the supply chain. In this regard the guidance is extensive and includes that third parties should be checked against the following:

1. Incident management
2. Business continuity and disaster recovery
3. Processes and procedures
4. Co-location and back up facilities
5. Internal assessments conformance to own policies
6. Information of performance and effectiveness in the above areas

As for data security, the first noticeable criticism is that it considers security generally and would not be suitable for the unique security considerations of governments placing sensitive data in the public cloud. However, the guidance does recognise that due to regulation and jurisdictional issues the physical location of the data is very important as well as by who and how the data is accessed, all of which are relevant to governments.

Overall the CSA Guidance itself does point out the fact that it will not be suitable for all situations due to the numerous cloud solutions available and that there cannot be a single list of security controls for all situations, for example governments will be faced with choices such as whether to use SaaS, PaaS or IaaS and private or public clouds.

2) **Cloud Control Matrix**

Established by the Cloud Security Alliance (CSA) the Cloud Control Matrix (CCM) is a set of security principles intended for both customer and provider and is primarily concerned with

assessing the security risk of a cloud provider. The CCM places an emphasis on information security control and offers guidance to both parties. The CCM is comprised of 16 domains which include Application and Interface Security, Business Continuity Management, Data Security and information Lifecycle Management, Data Centre Security, Governance and Risk Management, Human Resources Security, Identity and Access Management and Supply Chain Management, Transparency and Accountability. One of the useful attributes of the CCM is that all domains are cross referenced to other frameworks, standards and regulations that are widely recognized in this industry in order to provide ease of auditing. Another advantage of the CCM is that it normalises security expectations and simplifies terminology.

Although not developed specifically for the public sector, the CCM is the best option for governments when considering the public cloud until a cloud standardization roadmap becomes available. The problem is that there is a need to provide transparency in public sector cloud certification and the CCM is the answer. Dunne (2014) says that because the CCM maps well to other industry standards which includes ISO27001, and works well with the CAIQ in building a robust view of risk in the cloud.

However, evidence of the fact the CCM is not a complete solution for public sector cloud procurement is that it should be combined with another standard in order to ensure a high level of assurance, this has been recommended by Dunne (2014) who suggested that CCM can be combined with the UK's G-Cloud in order to offer an outstanding level of assurance. The G-Cloud element of this combination will cover the issue of governments placing sensitive data in the public cloud because it couples the sensitivity of the data with specific controls and evidence that must be provided by the cloud provider about how the data will be kept safe.

3) Consensus Assessment Initiative Questionnaire

The Consensus Assessment Initiative Questionnaire (CAIQ) is complementary to the CCM and the CSA Guidance and needs to be used in conjunction with these documents. It is a questionnaire that can be used by a customer to ask a cloud provider questions. The questions are based on the CCM. Not only does the CAIQ offer customers a way of creating an assessment process but it also allows the cloud provider to assess their own security.

4) ENISA

The next inevitable step for governments is to take further advantage of the public by using it for sensitive data. Unfortunately, until now the issue of protecting sensitive data in the public cloud has not been resolved. According to ENISA (ENISA, 2015) this is the reason that governments are apprehensive about putting sensitive data in the cloud.

The 'Security Framework for Governmental Clouds' developed by the European Union Agency for Network and Information Security (ENISA, 2015) is a practical frameworks and is based on the Plan Do Check Act model and is useful for governments who want to implement advanced

continuity to plan, implement and check what they have done. It includes a 14 point plan for government in the cloud, which includes verifying assurances about security from cloud providers, termination of contracts and deletion of data. Importantly, the ENISA framework recognises that the only way forward for governments to place sensitive data in the public cloud is either through a technical solution for enhanced security or a special SLA relationship with the cloud provider. The framework is applicable to all types of cloud solution including private, public and hybrid clouds and does not focus on the issues that arise with the public cloud specifically.

5) NIST

There are number of different versions of NIST which are addressed collective, except where noticeable differences are significant. NIST is an American standard under the FedRAMP. The standard offers privacy and security controls for government IS in the US. Where this standard is different to those offered by CSA is that it is intended for government but due to its comprehensiveness it can be applied to all information systems.

In addition to providing controls that are designed to protect operational functions, it is also designed to consider protection from cyber-attacks, natural disasters and system failures.

One of the main advantages of NIST in relation to this study is that it offers guidelines for security and privacy in the public cloud. For a government to use the public cloud then they would have to be offered a tailored solution from the cloud provider, the NIST standard offers guidance on the issues of non-negotiated or negotiated service level agreements (SLAs), the latter will allow governments to negotiate data ownership rights, vet employees, being notified of breaches, the segregation and encryption of data, isolating tenant applications, reporting of service effectiveness and compliance with laws and regulations, all of which are necessary not only for government in the public cloud with sensitive data but for long term continuity considerations as well.

NIST is also critical of a public cloud solution and warns against the fact that because it is a complex computing environment it allows for more opportunities for attack, that the public cloud is a shared multi-tenant environment where there is no physical separation which leaves it vulnerable to attack from within, and the fact that there is loss of control because unlike non-cloud solutions, risks are compounded by the fact that there external control over data assets, in other words governments lose governance over data. Other loss of control issues acknowledged by NIST are a lack of a point of contact so there is loss of control over computing decisions and a lack of coordination to ensure compliance with laws and regulations.

The main criticism of NIST is that it is applicable to all information systems including the cloud, and in consideration of the need to assess a cloud provider for suitability to offer a public cloud solution with sensitive data and possibly a digital continuity solution on a long term basis, NIST addresses all external providers of information technology, not just cloud providers. In fact, in reference to the relationship with a provider of the public cloud NIST clearly states that '*Although*

cloud computing is a new computing paradigm, outsourcing information technology services is not. The steps that organizations take remain basically the same for public clouds as with other, more traditional, information technology services, and existing guidelines for outsourcing generally apply as well'. However, NIST does recognise the increased complexity of achieving oversight for maintaining control and accountability where responsibility of is handed over to the provider of the public cloud.

K. Overall Criticisms of CSFs

There are a number of criticisms that are applicable to the FSCs generally that will have implications for their suitability for government. Here these criticisms are addressed.

1) Multiple Jurisdictions

Data protection legislation is often cited as one of the main concerns in the adoption of the cloud, this is due to the fact that cloud computing is borderless involving many jurisdictions that have different laws, and according to the European Union Agency for Network and Information Security (ENISA) there are few standards or certification available that address compliance needs of cloud users in respect to the issue of multiple jurisdictions. Thus, there is a need for FSCs that assure governments that they will be compliant not only with international laws, but also their own laws when using the public cloud (ENISA NOV 2014).

2) Too Many FSCs

Although there are many FSCs that have lot in common, there are also differences between them meaning that not one standard exists that covers all situations, moreover, the issue of having to many FSCs also raises the question of which one should be followed, although it should recognized that many security standards in cloud computing and set an example for security standard generally (Duncan and Whittington, 2014). The numerous standards which include among others ARTS, CSA, CSCC, DMTF, ENISA, ETSI, FedRamp, GAPP, GICTF, ISO, ITU, NIST, OASIS, OCC, OGF, OMG, PCI or SNIA creates a degree of confusion and there is no one-size-fits-all approach (Duncan and Whittington, 2014).

3) Reactive and Late

FSCs are often reactive in nature which means they are always one step behind the developments in cloud computing and there will always be a lead time between decision making and implementation. To make this reactivity and lateness more complex for international standards different countries have different agendas and there are continuous technological changes (Duncan and Whittington, 2014). Another problem in this area is that many security standards were developed before the evolution of cloud computing, for example the NIST SP800-53 standard (Duncan and Whittington, 2014).

CONCLUSION

One of the main findings of the study is that although there are numerous FSCs available, there is not one standard that is suitable for the specific situation of a government using a public cloud solution for sensitive data with the provision for advanced digital continuity whereby a government can operate from the cloud indefinitely in the case of a disaster. However, between the different FSCs a number of these aspects are covered, for example there are FSCs that are designed for government use and consider the issue of sensitive data, there are also number of FSCs that emphasise consideration of the issue of governance, something that is pertinent to governments because they are bound by laws regarding the protection of data.

In order for governments to have confidence in the public cloud for sensitive data and advanced digital continuity it is necessary to have a new standard specifically for this purpose, this will not only offer a solution that will guide governments, but also overcome the limitations of the FSCs in terms of the fact that they do not consider the issue of multi jurisdictions which is essential for governments and the fact that they are reactive and late where a solution is needed that is ready for the latest development of government in the cloud.

REFERENCES

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

[2] M. Aziz, J. Abawajy, M. Chowdhury (2013). The Challenges of Cloud Technology Adoption in E-Government. *2013 International Conference on Advanced Computer Science Applications and Technologies*, 470 - 473.

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

[4] M .Deman, D. Vintar, (2013),"A possible solution for digital preservation of e-government", Aslib Proceedings, Vol. 65 Iss 4 pp. 406 - 424

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

[6] B. Duncan, B. & M. Whittington. 2014, "Compliance with standards, assurance and audit: Does this equal security?" in Vol 2014-. ; 2014.

[7] M. Dunne. (2014). Cloud Security Alliance And Government Cloud. e forensics magazine. 3 (4)

[8] ENISA. (2015). Security Framework for Governmental Clouds.European Union Agency for Network and Information Security, 1 -34.

[9] ENISA. (2011). Security & Resilience in Governmental Clouds - Making an informed decision. ENISA., 1 - 141.

[10] S. Hashemi. (2013). Cloud Computing Technology For Egovernment Architecture. International Journal in Foundations of Computer Science & Technology. 3 (6), 15 - 23.

[11] K. Hashizume, D.G. Rosado, E. Fernández-Medina & E.B. Fernandez. 2013, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1-13.

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

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

[14] J. Luna, H. Ghani., D. Germanus & N Suri. 2011, "A security metrics framework for the Cloud", INSTICC, , pp. 245.

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

[16] O. Rebollo, D. Mellado, & E. Fernandez-Medina. 2012, "A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment", *JOURNAL OF UNIVERSAL COMPUTER SCIENCE*, vol. 18, no. 6, pp. 798-815.

[17] Scotland. (2014). Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector. Digital Scotland, 1 - 39.

[18] 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.