Journal of Innovation Information Technology and Application (JINITA)
Vol.4, No.1, June 2022, pp.82-92
DOI: doi.org/10.35970/jinita.v4i1.1292

Information Security Governance Framework in Public Cloud a Case in Low Resource Economies in Uganda

Fredrick Kanobe *[1], SP Sambo [2], Billy Mathias Kalema[3]
[1]Kyambogo University (KYU), School of Computing and Information Science, Uganda
[2]Tshwane University of Technology (TUT), Department of Informatics, Uganda
[3]University Mpumalanga Sciences (UMP), School of Computing and Mathematical Sciences, South Africa
e-mail : fkanobe@kyu.ac.ug[1], samanthasambo2@gmail.com[2], billy.kalema@ump.ac.za[3]

Abstract

The study aimed at exploring the critical enablers to the development and usage of information security governance frameworks for cloud computing in Uganda. The study was motivated by the continuous information security governance challenges in the Public Cloud. The theoretical frameworks that underpinned this study included; Contingency management theory, the Risk Management framework, the Technological Organisational and Environmental (TOE) model and the Information Security Governance model. This study adopted a quantitative research approach to obtain data through a survey. Five key factors for information security governance were identified: a) Technological factors: flexibility, scalability, availability, agility, data protection governance, trust of cloud, data source, maintenance, data retention and policy. b) Organisation: size and structure of the organisation, top management support. c) Environmental factors: governance and regulation, marketing, vendor, resource availability, obsoleteness. d) Individual: user resistance, attitude, skills, belief and learnability. e) Risk management and control factors: risk assessment, disaster recovery, access and authorisation control, monitoring, auditing, and process risk control. The study contributes to theory and practice in information security. The developed framework and its accompanying model helped to inform public departments, organisational top management and information security strategies to avoid excessive information risks and potential regulatory compliance failures in public cloud. The study was inclined on subjective information security, which alone may not fully address all information security problems in a public cloud. Therefore, it is recommendable that future research studies on objective security in public cloud.

Keywords*: Cloud computing, cloud security governance, computer security, information security*

Introduction

Cloud computing continues to grow in popularity as one of the new innovations in computing that globally has attracted the attention of many industries. This is because cloud computing is very convenient and avails on-demand computer network access to a centralised pool of Information Technology (IT) resources that can hastily be deployed with minimal management overhead. There are four main types of cloud computing namely private clouds, public clouds, hybrid clouds, and community or multiclouds. The benefits of cloud computing are not limited to the provision of cost effective services, ease of use, flexibility but also enhance optimal sharing of IT resources [1;2]. This has compelled many organisations and individuals to relocate their Information and Communication Technology (ICT) resources to the cloud-computing environment.

[3] emphasise that cloud computing has not only become an option of choice for institutions, organisations but also for personal use because of timely availability of information, cost effective storage space and easy accessibility of data hence enabling its users to access it any time anywhere globally. Public cloud is the most commonly adopted type of cloud computing because it avails cloud model services to the public on a pay-as-you use term and usually governed by the supplier [4]. Whereas the provision of the public cloud through public Internet comes with various benefits, it also poses security challenges to the end-users. The availability of the public cloud open access can lead to many information security risks and challenges that require security control measures and governance. The public cloud computing poses a number of challenges such as public auditing, applications, information systems, communication, virtualization, data

*) Corresponding Author : fkanobe@kyu.ac.ug

availability and integrity issues, data security, administrative security that all result into security breaches [5; 6]. Therefore, the need for security governance of public cloud is beyond debate lest the tremendous benefits of the cloud computing to the end-users are eroded.

The absence of security governance in the public could not only worries its users but also opens doors for cyber-attacks, data leakage and may minimise privacy, confidentiality and integrity of data. [7] maintains that information security functions with good organisation business strategies can lead to reduction of security risks to an acceptable level and improve performance management in organisations. There has been some efforts to develop cloud security standards. [8], however, maintain that most cloud providers are implementing cluttered security, leading to uncertainty for cloud consumers. The great cloud computing innovations continue to receive negative observations by various scholars.) Those who have attempted to deal with cloud computing security pay little attention to the governance aspects ([9; 10; 11]. Therefore, there is still need for an appropriate framework to inform public cloud governance. The main goal of the study was therefore to explore the critical factors needed to develop a framework for security governance in the cloud environment in a low resource economy country with a focus on Uganda.

Cloud Computing Models

Cloud computing is one of the new development trends of technology that offers an innovative business model for organisations to adopt without upfront investment [12]. Cloud computing services are gaining rapid adoption in firms seeking cost reduction, technical expertise, flexibility and gain competitive advantage in the fast developing business environments. The cloud computing technology traditionally provides various cloud delivery infrastructure models namely Software as a Service, Platform as a Service and Infrastructure as a Service [13;14].

Software as a Service (SaaS): the SaaS service model is a platform for offering software services to users [14]. The model provides users with some basic benefits such as authentication for safe communication, authorization control and a secure data storage. *Infrastructure as a Service (IaaS):* The IaaS service model is a platform for offering infrastructure services such as storage, network components and servers [15]. The IaaS provides tools such as firewalls and load balancing the system. Unlike the other service models, the security vulnerabilities that may occur in virtualization governance are likely to be less as the IaaS process is better controlled. *PaaS as a Service (PaaS):* The PaaS service model offers applications and development tools for users [3]) The user is given options for storage, management and to construct his or her own particular applications which run on the third parties' base.

Business Process Management as a Service (BPMaaS): The BPMaaS service model provides the complete end-to-end business process management required for the creation of unique business processes [15]. A summarized description of business process management can be formulated as corporate business process optimization and management over the integrated network and single systems such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) or Supply Chain Management (SCM). BPM system has the assignment to coordinate the execution of a business process step-by-step by means of monitoring, evaluating and identifying where business processes crash or do trouble. *Business Process as a Service* (BPaaS): BPaaS is an approach to make a company's workflow more effective, efficient and adjustable to new developments and frame conditions[16]. The workflow enables businesses to be more flexible and provides an advantage of decreasing their spending. *Database as a Service (DBaaS):* This is a service model in cloud computing that provides automated services where consumers can request database-oriented functions from a dedicated service hosted on the cloud [17]. Customer self-service interaction model as organisations are allowed to use, configure and deploy the cloud database services themselves without any IT support and without purchasing any hardware for specific people.

Table 1: *Cloud Implementation challenges*

Author /Year	Study	Implementation Challenges
[18]	Data access control in the cloud computing environment for bioinformatics	• Transferability • Security • Privacy
[19]	Data control in public cloud computing: Issues and Challenges	• Security mechanism • Data breaches • Data security
[20]	Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models	• Lack of governance
[21]	Information security governance frameworks in cloud computing an overview	• Information security risks
[22]	Cloud computing implementation, management and security.	• Fear of an unknown variable • Changes to current control procedures
[15]	A Comparison of IT Governance and control frameworks in cloud computing	• Trust and security.

Cloud security governance

Cloud security governance entails putting in place and enforcing policies, procedures and standards in order to prevent potential threats, hacks and loss of information [23]. The absence of information security control and guides in the cloud environment results into mistrust. This implies that protection of information in the cloud is a key consumer concern and a determinant key factor for migrating to the cloud environment. [24] maintain that security of the cloud platform has become a key research domain in the academia hence leading to several empirical studies. Organisations need to recognise that securing information is not just an investment, but it is essential for survival of all cases and, for many, it can even create competitive advantage once its security.

Methodology and Theoritical Framework

This study utilized several theoretical frameworks to formulate a comprehensive theory to analyse cloud security of the existing governance framework for cloud computing in Uganda which included; the Technology Organisation Environment Theoretical framework (TOE), the Contingency Management Theoretical Framework (CTF), the Risk Management and the Information Security Governance (ISG).

Technology Organisation Environment Theoretical Framework - In the context of this theory, [25] state that the context of technology, organisation and environment has an influence in the development of a cloud service adoption, pricing mechanism and deployment cloud models. [4], however argue that cloud cost savings; availability, scalability and flexibility have given cloud computing gain competitive advantage to several organisations over those outside the cloud. *Contingency Management Theoretical Framework* – Developed by [26], the theory places information security governance as part of contingency management. The constructs that were used in this theoretical framework are integration, low cost, development and supportability.

Risk Management Theoretical Framework (RMRF) - The Risk Management Theory developed by [27] seeks to uncover the multitude of challenges managers face as they seek to acquire cloud technology for their organisations. Three risks related to services, technology and process risks were identified. RMRF helps managers to identify their organisations general risk profile and link that profile to a specific configuration of resolutions. *Information Security Governance Theoretical Framework (ISG)* - The ISG prescribes the policies that support security model. Policy issues are the responsibility of top management in organisations. Therefore, information security should be addressed from an executive level. [28] explain that information security governance is an important factor for all organisations seeking to adopt cloud computing. Given the value of information technology resources, there is an increasing concern for security

governance in the cloud.

Conceptual Model

A conceptual model was developed from the theoretical foundation as depicted in figure 1.

Hypotheses development

a) Technology was categorized into two sub constructs thus technological characteristics and preparedness for the cloud forming Hypothesis H1 and its sub hypotheses H1a and H1b.

H1: Technology factors when moderated by risk management and control influence cloud security governance.

H1a: Technology factors due to technological innovations characteristics when moderated by risk management and control influence cloud security governance.

H1b: Technology factors due to organisational preparedness when moderated by risk management and control influence cloud security governance.

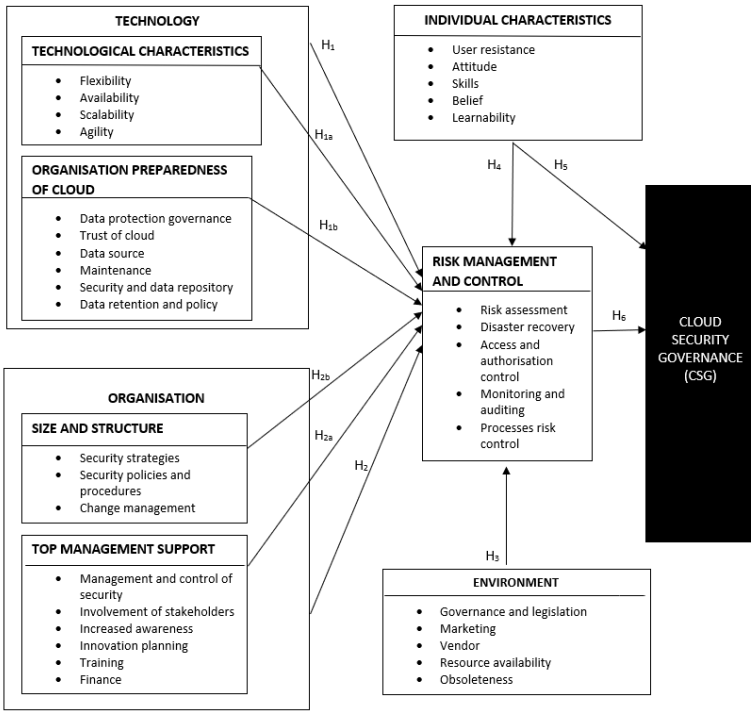

Figure 1: *Conceptual Model*

b) Organisation factors was classified into two sub-constructs namely organisation size and structure forming Hypothesis H1 and its sub-hypotheses H2a and H2b.

H2: Organisational factors when moderated by risk management and control influence cloud security governance.

H2a: Organisational factors due to the size and structure of the organisation when moderated by risk management and control influence cloud security governance.

H2b: Organisational factors due to the top management support when moderated by risk management and control influence cloud security governance.

c) Environment which refers to the surroundings of the organisation that is implementing a public cloud formed the third hypothesis for the study.

H3: Environmental factors when moderated by risk management and control influence cloud security governance.

d) Individual characteristics involving user resistance, attitude, skills, beliefs and learnability

formed the fourth hypothesis. The fifth hypothesis was developed based on a direct influence between individual factors and cloud security governance.
H4: Individual characteristics when moderated by risk management and control influence cloud security governance.
H5: Individual characteristics has a direct influence on cloud security governance

e) The last construct was risk management and control which was hypothesized to have a direct influence with cloud security governance. Based on this construct a sixth hypothesis was developed.
H6: Risk management and control has a direct positive influence on cloud security governance

Research Design and Methods

This study followed a quantitative research approach to collect data from government departments in Uganda using a questionnaire with close-ended questions. The study respondents were selected using simple random sampling by using the [29] tool for determining sample sizes for finite population. Out of the target population of 500 respondents, a sample size of 217 was used. These were senior government officials who are involved in ICT activities. The data analysis procedures comprised of processing, synthesizing and interpretation. Both descriptive and inferential statistics were used whereby descriptive statistics were used to analyse the frequencies of the research respondents' demographics and situation variables while inferential statistics was used to determine the casual relationships between constructs and their prediction power to the cloud security governance. The overall reliability statistics based on the Cronbach Alpha coefficient was 0.929 measured on 46 items, a value above the acceptable value of 0.7.

Results and Discussions

Results

Pearson Correlation of the constructs

[30] allude that the Pearson correlation of constructs is a form of design research in which an examiner measures and set out the degree of a relationship between two or more constructs. This method is used to measure the association between continuous variable which are both dependent and independent. Additionally, the method can be either positive or negative. The positive correlated variable implies that as value one increases, the other variables also increase; whereas the negative correlation implies that when the value of one variable increases then the value of the other decreases. [31] state that the correlation coefficient values ranges from -1 to 1 where -1 is perfect negative relation and 1 is a perfect positive relation. In this study, a Pearson's correlation method was used to signify the relationship between constructs.

Table 2 below discloses grouped factors that have a positive and highly significant correlation with one another. The table shows that technological factors have significant relationship of .546 (2-tailed) with one another. Organisational size and structure factors also have a significant relationship with technology organisational preparedness at the 0.01 level .293 (2-tailed), and oragnisational size and structure at .557 (2-tailed). However, the organisational size and structure and technological characteristics have an inverse relationship with perceived ease of use of -.027. Organisational top management support has a significant relationship with technological factors and organisational factors with the most significant correlation between organisational top management support and size and structure of .445 (2-tailed). Environmental factors have the most significant correlation coefficient with organisational top management support with a correlation-value of .568 that is significant at the 0.01 level (2-tailed). Additionally, the table shows that there is a significant correlation amongst individual characteristic constructs at the 0.01 level (2-tailed). This implies that individual characteristics have influence where cloud security governance is concerned. It further exposes that individuals do not see much support

from top management in relation to cloud security governance. This might be the reason that cloud computing is relatively a new concept. Risk management and control factors have the most significant correlation coefficient of .859 that is at the 0.01 level (2-tailed). Regression analysis is a very powerful technique used in statistical analysis to study the relationship between two or more variables [30]. While there are different types of regression analysis, their core objective is to examine the relation of one or more independent variable with a dependent variable. Based on the regression analysis, it is possible to determine the contribution of an independent variable towards the overall prediction of the model

Table 2: Demonstration of the relationship between constructs used in this study

		Techar	TechRC	OrgSS	OrgTMS	Envt	INDchar	RiskMgt	CGS
Person Correlation									
TechChat	Sig.(2 -tailed)	1							
	N	128							
	Person Correlation	.546**	1						
TechRc	Sig.(2 -tailed)	.000							
	N	128	128						
	Person Correlation	.024	229**	1					
OrgSS	Sig.(2 – tailed)	.787	.099						
	N	128	128	128					
	Person Correlation	.-027	.293**	.557**	1				
OrgTMS	Sig.(2 –tailed)	.766	.001	.000					
	Person Correlation	0.66	.192*	.455**	.361**	1			
Envt	Sig.(2 –tailed)	.456	.030	.000	.000				
	N	128	128	128	128	128			
	Person Correlation	.094	.370*	.458**	.568**	.361**	1		
INDChar	Sig.(2 –tailed)	.290	.000	.000	.000	.000			
	N	128	128	128	128	128			
	Person Correlation	.094	.285”	.352”	.431”	.356”	.689”	1	
RiskMgt	Sig.(2 –tailed)	0292	000	000	000	000	000		
	N	127	127	127	127	127	127	127	
	Person Correlation	.062	.198*	.197*	.264**	.271**	.343**	*859**	1
CGS	Sig.(2 –tailed)	.485	.025	.027	.003	.002	.000	.000	
	N	127	127	127	127	127	127	127	127

** Correlation is significant at the 0.01 level (2-tailed).
*Correlation is significant at the 0.05 level (2-tailed)

Table 2: illustrates the overall prediction of the model for cloud security governance to improve competitiveness in government institutions.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	Df1	Df2	Sig F Change
1	.928[a]	.861	.853	.29333	.861	105.158	7	119	.000

The results in Table 3 indicate that the overall prediction of the conceptual framework for cloud security governance to improve competitiveness in government institutions is 86.1% (R2 = .861). This implies that the integration of the TOE framework, risk management and the individual variables contribute 86.1% to the prediction of competitiveness when cloud security governance is effectively analysed.

Table 3: Illustration of the Coefficients of each framework

Framework		Unstandardized Coefficients		Standardized Coefficients	t	Sig	Collinearity Statistics	
		B	*Std. Error*	*Beta*			*Tolerance*	*VIF*
1	(Constant)	.112	.018		6.246	.000		
	TechChar	.160	.055	.138	2.911	.036	.658	1.521
	TechRC	.176	.052	.162	3.379	.011	.571	1.753
	OrgSS	.179	.060	.137	2.827	.041	.600	1.666
	OrgTMS	.131	.065	.129	1.993	.045	.540	1.852
	Envt	.054	.051	.042	1.059	.292	.745	1.342
	INDVChar	.271	.062	.502	4.385	.000	.408	2.499
	RiskMgt	.288	.062	.577	4.650	.000	.513	1.949

a. Dependent Variable: CSG

Based on the regression and correlational analysis, the set hypotheses were tested and the results are presented in Table 5.

Table 4: Testing of Hypothesis

Hypothesis	Results	Action
A. Technology Factors		
H_0: Technology factors due to technological innovations characteristics when moderated by risk management and control influence cloud security governance.	P = .036< 0.05	retained
B. Organisational Factors		
H_0: Organisational factors due to the size and structure of the organisation when moderated by risk management and control influence cloud security governance.	P = .041 < 0.05	Retained
Environmental Factors		
H_0: Environmental factors when moderated by risk management and control influence cloud security governance.	P = .292 < 0.05	Retained
Individual Factors		
H_0: Individual characteristics when moderated by risk management and control influence cloud security governance.	P = .000 < 0.05	Retained
Risk Management Factors		
H_0: Risk management and control has a direct positive influence on cloud security governance	P = .000 < 0.05	Retained

Discussions

The study focused on determining factors that influence security governance in the public cloud environment in low resource economies taking a case of Uganda. A broad literature review was undertaken and discussed. Additional factors were identified in the related models. These factors were categorised as technological, environmental and organisational, individual, risk management and control. Analysis of the study revealed that 3factors had impact on information security governanceframeworks for cloud computing in Uganda. Based on this categorization and analysis, the following technological factors were significant.

1 Flexibility
2 Scalability
3 Availability
4 Agility
5 Data protection governance
6 Trust of cloud
7 Data source
8 Maintenance
9 Security
10 Data retention and policy

In the organisational category, the following factors were significant:

1) Size and structure of organisation
2) Top Management support

The following Environmental factors were found significant;

1) Governance and legislation
2) Marketing
3) Vendor
4) Resource availability
5) Obsoleteness

The Individual category, the factors that were significant include;

1) User resistance
2) Attitude
3) Skills
4) Belief
5) Learnability

Lastly, the risk management and control factors that were significant;

1) Risk assessment
2) Disaster recovery
3) Access and authorisation control
4) Monitoring and auditing
5) Process risk control

The study aimed at exploring the critical factors needed for the development of information security governance framework for cloud computing in Uganda. Based on the findings the developed framework is represented in figure 2.

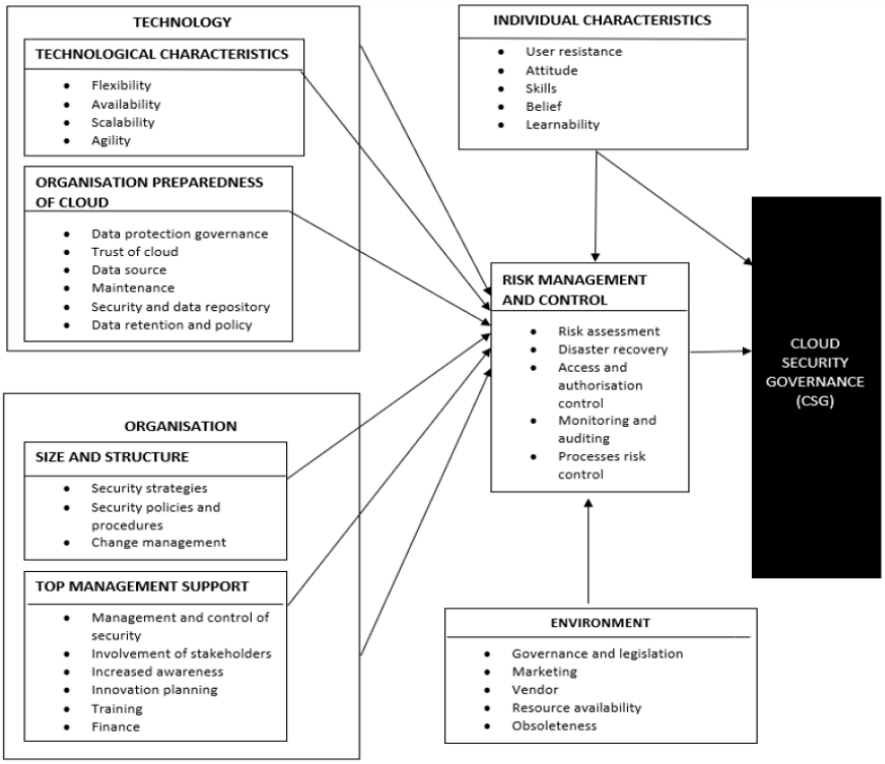

Figure 2: Information Security Governance Framework in Public Cloud for low resource economies

Technology factors when moderated by risk management and control positively influence cloud security governance. This hypothesis was retained at level of significant 0.36. Technology denotes internal and external technologies consequently, acceptance of technology depends on its expected benefits and compatibility in the existing environment [32]. This implies that technological factors are important for acceptance of innovation. The attributes of technological innovations define how well an innovation can be developed to fit the contemporary system and support to functional and non-functional requirements. Needless to mention the technological innovation attributes are obligatory for users to distinguish between usefulness and ease of the technology. Organisation's IT infrastructure require to have attributes of flexibility, scalability,

availability and agility for a successful cloud technology acceptance.
Organisational factors due to the size and structure of the organisation when moderated by risk management and control positively influence cloud security governance. This hypothesis was retained at level of significance 0.41. The severity of security risks in most cases are associated to the size and structure of the organisation. A good organisation structure provides quick reporting and response to information security incidents. In order to acquire a holistic framework for cloud security governance, the presence of systematic organisational structures is important [33]. Organisational factors entails top management support comprises management and control of security, stakeholder involvement, innovation, planning, training and appropriate resource allocation. Top Management support can contribute to the acceptance of innovations and security governance. [31] note that top management through most appropriate resource allocation promotes information technology governance.
Environmental factors when moderated by risk management and control positively influence cloud security governance. This hypothesis was retained at level of significance 0.292. Environmental factors when moderated by risk management and control, such as governance and legislation, marketing, vendor, resource availability and obsoleteness have an influence on cloud security governance. [34] state that competition, compatibility, environmental pressures, and government support have a positive impact on organisational readiness for cloud computing.
Individual characteristics when moderated by risk management and control influence cloud security governance. This hypothesis was retained at level of significance 0.00. Individual characteristics have a direct influence on cloud security governance. Individual attributes such a user resistance, attitude, skills, belief and willingness to learn the technology, is paramount for attaining self-efficacy that leads to ease of use of technology and its effective management and control to security. This implies that building personnel knowledge such as awareness and the knowledge of governing the technology strengthens the security of the cloud. This is because sometime, ignorance and lack of awareness of security risks and threats lead to vulnerability of the cloud environment. [35] state that employees' detailed understanding of an organisations operational routines and procedures results into improved management and control security challenges in the cloud.
Risk management and control has a direct positive influence on cloud security governance. This hypothesis was retained at level of significance 0.00. [36] disclose that risk management and control has a direct positive influence on cloud security governance. The researchers indicate that there are no comprehensive models available to help managers assess and mitigate the risks they face in terms of cloud security governance. Three types of risks are associated with this factor and they include services, technology and process risks with four types of resolutions; stakeholder engagement, technology development, innovation planning and innovation control. This will help managers identify their organisation's general risk profile and link that profile to a specific configuration of resolutions

Recommendations and Conclusion

Recommendations

Organisations implement many different technology strategies to remain competitive in their respective industries. This study developed a security governance framework for a public cloud in low resource economies. This study focused on subjective information security, which may not sufficient to address information security challenges in the public cloud. It is recommendable that objective information security in the cloud and more especially in low resource economies be given attention too as additional area of future research.
This study used simple random sampling for data collection and the results reported were based on inferential statistics involving correlation and regression from which the conclusion was made. The data were collected at one period using a cross-sectional dimension. However, individual characteristics towards technology may vary depending on time changes. It is, therefore,

recommended that a longitudinal study should be conducted to examine individuals' characteristics with change in time.

The framework presented in this study was based on public cloud security governance factors. However, different organisations may have varying challenges and levels of technology usage and governance may differ. This may limit the generalisation of the findings to other various economies; the fact the study did not include the validation of the framework. A comparative study between high resource economies is recommend as this study focused on low recourse economies to compare findings with this study. Further, it is recommendable that a future study to validate the framework is conducted before it can be fully and effectively used for security governance of the public cloud.

Conclusion

Regardless of the technology deployment in cloud computing, its security governance is a key success factor for its acceptance. The findings of this study shows that individual, technological and environmental characteristics, top management support, organisation's preparedness, organisation size and structure, risk management and control play a vital role security government of the cloud. Cloud computing will continue to gain popularity because of its reduced operational costs, flexibility, ease of access to a pool of computer resources making end-users attain competitive advantage. The developed framework makes a significant contribution to information security practices, standards and management.

Reference

1) M. Ali, S.U. Khan and A.V. Vasilakos, "Security in cloud computing: Opportunities and challenges", *Information Sciences,* vol. 305, no. 1. pp.357-383, 2015.
2) A. Botta, W. De Donato, V. Persico,V & A. Pescapé, "Integration of cloud computing and internet of things: a survey", *Future Generation Computer Systems,* Vol. 56, no. 3, pp 684-700, 2016.
3) M.Y.Y. Yesilyurt, "New approach for ensuring cloud computing security: using data hiding methods", *Idian Academy of Sciences,* vol. 41, no. 11, pp 1289–1298, 2016.
4) O.Al-Hujran, E.M. Al-Lozi, and M.M.Al-Debei. "Challenges of cloud computing adoption from the TOE framework perspective", *International Journal of E-Business Research (IJEBR),* vol. 14, no. 3, *pp. 77-94,* 2018.
5) U. Gupta, S. Saluja, S and T. Tiwari, "Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms", *International journal of Recent Research Aspects,* vol. 5, no. 1, Pp.55-61, 2018.
6) D. Puthal, B. P. S. Sahoo, S. Mishra and S. Swain, "Cloud Computing Features, Issues, and Challenges: A Big Picture," in *2015 International Conference on Computational Intelligence and Networks,* pp. 116-123 , 2015.
7) A.C. Khurram, "Research Analytics: A Practical Approach to Data analysis Paperback", India: Wiley, 2017.
8) R. Kalaiprasath, Elankavi R. and R. Udayakumar, "Cloud Security and Compliance - A Semantic Approach in End to End Security", *International Journal on Smart Sensing and Intelligent Systems*, vol. 10, 482 – 494, 2017.
9) M. Jouini and L.B. Rabai, "A Security Framework for Secure Cloud Computing Environments", *International Journal of Cloud Applications and Computing (IJAC),* vol. 6, no. 3, 32-44, 2019.
10) O. Rebollo, D. Mellado & J. Fernández-Medin, "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, 2013.
11) P.J. Schmidt, A.J. Steele and S.V. Grabski Schmidt, "Business in the Cloud: Research Questions on Governance, Audit, and Assurance." *J. Inf. Syst,* vol. 30, pp.173-189, 2016.
12) M. Almorsy, J. Grundy,and I., Müller , "An analysis of computer science problem", arXiv preprint arXiv:1609.01107, 2016.
13) D. C. Marinescu, Cloud Computing Theory and Practice, Second Edi. Cambridge: Morgan Kaufmann Publishers, 2018.
14) J. Sen, "Security and privacy issues in cloud computing." In Cloud Technology: Concepts, Methodologies, Tools, and Applications, IGI Global pp. 1585-1630., 2015.

15) E. Bailey and J.D. Becker, "A comparison of IT governance and control frameworks in cloud computing", *in Twentieth American Conference on Information Systems, Savannah*, 2014.
16) D. Paschek, A. Trusculescu and A. Mateescu, "Business process as a service - a flexible approach for it service management and business process outsourcing", *Management, Knowledge and Learning International Conference 2017 Technology, Innovation and Industrial Management*, 2017.
17) K. Munir, "Security model for cloud database as a service (DBaaS)", in *International Conference on Cloud Technologies and Applications (CloudTech), pp. 1-5, 2015.*
18) S. Namasudra, "Data Access Control in the Cloud Computing Environment for Bioinformatics", *International Journal of Applied Research in Bioinformatics (IJARB)*, vol. 11, no. 1, 2021.
19) A. Sharma, P. Jha, and S. Singh, "Data Control in Public Cloud Computing: Issues and Challenges", *Recent Advances in Computer Science and Communications*, vol. 14, no. 2, pp.c564-579, 2021.
20) Y. Bounagui, A. Mezrioui and H. Hafiddi, "Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models", *Comput. Stand. Interfaces*, vol. 62, pp. 98-118, 2019.
21) M. Al-hashimi, M. Othman, H. Sulaiman and A. A. Zaidan, "Information Security Governance Frameworks in cloud computing an overview". *Journal of Advanced Computer Science and Technology Research*, vol. 8 no. 2, June 2018, pp. 67 – 81, 2018.
22) J.W. Rittinghouse, J.F. Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, Boca Raton, 2010
23) P.J. Schmidt, A.J. Steele, & S.V. Grabski, 2017: Cloud Computing: Governance and audit research questions. Washburn University, School of Business.
24) V. Jaglan and V. Jaglan, "Proposing Efficient Approach to Improve Integrity Checking in Cloud Data Security", *International Journal of Recent Research Aspects*, vol. 2, Issue 3, September 2015, pp. 125-129, 2015.
25) P.F. Hsu, S. Ray and Y.Y. Li-Hsieh, "Examining cloud computing adoption intention, pricing mechanism, and deployment model", *International Journal of Information Management*, vol. 34, no. 4, pp. 474-488, 2014.
26) R. Drazin, and A.H.Van de Ven, "Alternative Forms of Fit in Contingency Theory." *Administrative Science Quarterly*, vol. 30, no. 4., pp. 514-539, 1985.
27) K.M. Klimczak, "Risk Management Theory: A Comprehensive Empirical Assessment", University Library of Munich, Germany, 2007,
28) R.S. Moghadam and R. Colomo-Palacios, "Information security governance in big data environments: A systematic mapping". *Procedia computer science*, vol. 138, pp. 401-408, 2018.
29) R.V. Krejcie and D. W. Morgan, "Determining Sample Size for Research Activities", *Educational and Psychological Measurement*, vol. 30, no. 3., pp. 607-610, 1970.
30) J.W. Creswell and T.C. Guetterman, "Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research, 6th Edition", Boston, MA : Pearson Education, 2018.
31) P. Schober, C. Boer, C. and L. Schwarte, "Correlation Coefficients: Appropriate Use and Interpretation", *Anesthesia & Analgesia*, vol. 126, no. 5., pp 1763-1768, 2018.
32) B.P. Borgman, B. Bahli and H. Heier, "Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework," in *2013 46th Hawaii International Conference on System Sciences*, 2013, pp. 4425-4435, doi: 10.1109/HICSS.2013.132.
33) M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance", *Personal and Ubiquitous Computing*. pp 1–21, 2018.
34) J. Malak, "An Analysis of the Technological, Organizational, and Environmental Factors Influencing Cloud Adoption", Ph.D. dissertation, Walden University, 2017.
35) T.P. Gunasekaran, R. Papadopoulos, SF. Dubey; SJ. Wamba, B. Childe, Hazel and S. Akter, "Big data and predictive analytics for supply chain and organisational performance", *Journal of Business Research*, vol. 70, pp. 308–317, 2017.
36) A. W. D. Ali, and L. Mathiassen," Cloud-base business services innovation: A risk management model", *International Journal of Information Management*, vol. 37, no.6, pp 639-649, 2017.