International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 359-365www.ijaem.net ISSN: 2395-5252

# Implementation of Cloud Computing Security Governance

Michael Oloche Ogbole[1], Engr. Adakole Lawrence Ogbole[2]

[1] *Information Security & Risk Officer, Eaglewings Network Solutions Ltd Lagos*
[2] *Groudp Head, Group Audit & Compliance, Unified Payment Services Ltd Lagos*

---------------------------------------------------------------------------------------------------------------------------------------
Date of Submission: 05-01-2021 Date of Acceptance: 07-01-2021
---------------------------------------------------------------------------------------------------------------------------------------

**ABSTRACT**: Cloud computing undoubtedly continue to attract businesses due to the advantages that it brings. Conversely, security challenges have been a long-lasting issue in the practice of Cloud Computing. Efforts have been made to tackle this security issues but failed as emphases were based on technical issues stemming from IT siloes procedures without support from the organization at large. With the increased cost-effective service offering of cloud computing and its adoption, cloud computing security governance is accruing interest amidst professionals but its implementation is shaggily researched. This paper presents a conceptual framework to securing cloud computing from governance perspective. The paper also discusses three steps to implementing effective cloud computing security governance.

**KEYWORDS:**Cloud computing, Security, governance, Framework.

## I. INTRODUCTION

The ubiquity of internet infused tremendous growth in cloud computing paradigm in the last decade. However, security has been a heinous bottleneck in this computing paradigm. Cloud computing extrapolates its services beyond the confine of corporate environment causing technical and non-technical risks to information asset. Hence the need for cloud computing security governance cannot be overemphasized. Cloud computing security governance describes how security can be effectively managed through active corporate strategic leadership. It entails participants in the hierarchy of (Board of Directors, Executives, Managers and Employees) in the domiciled organization and external participants such as end-users and third-parties. Further, to tackle security issues in cloud computing, its governance has to be considered to be an aspect of organizations' vast corporate governance strategy irrespective of the cloud computing model adopted. A cloud computing security governance conceptual framework is designed in this paper to show how functionalities of all participants should be aligned to enhance formidable security for cloud computing.

Furthermore, cloud computing is a new paradigm, its security is dynamic and the concept of security governance is still at infant stage (Sperling & Webber, 2019). This is the reason there exist different cloud computing security governance framework today. Again, cloud computing security governance has not attracted much research. The few available researches in the realm of academia and industry did not emphasize implementation of cloud computing security governance. Hence, this paper present significant work in this neglected research aspect. The next section presents relevant literatures in Cloud computing security governance. Section III proposes a conceptual cloud computing security governance framework, section IV entails effective implementation of cloud computing security governance with detailed steps and section V presents conclusion and future work.

## II. RELATED LITERATURES

The advent of cloud computing practices is accompanied with risks, vulnerabilities and threats. The "European Network and Information Security Agency" published 35 risks collated by 19 contributors and identified 8 most prominent risks on the basis of their likelihood of event and level of impact (ENISA, 2009). They provided guides in terms of technical, policies and legal compliance. Subsequently, the Open "Web Application Security Project" released ten utmost common cloud security risks, which was harnessed from other literatures (OWASP, 2011). The OWASP (2011) risks are contained in ENISA (2009) except that OWASP (2011) mentioned loss of governance as a consequence of risk. Conversely, ENISA (2009) listed vendor proprietary and malicious insider as devastating risks. While ENISA (2009) prescribed risk assessment and stringent service level agreement (SLA) as a solution, none of the literatures proffered solution to the risks through governance.

Furthermore, Hussein and Khalid (2016) in their research focused on the triggers that lead to vulnerabilities in cloud computing as well as virtual machines. Similarly, Mishra et al. (2013) also emphasised on virtualisation and multi-tenant attacks and also proposed fine segregation of the layers of cloud computing infrastructure such as: operating systems, hardware and virtual machines. Their proposed solutions are common practice that most industries have in place and are still suffering from security issues.

Again, in 2012, Ashktorab and Taghizadeh gave a comprehensive list of security threats in cloud computing and how to prevent them. However, the lists of the given threats are holistic and some of the threats can be mitigated by simple configuration or practice. For example, cookie poisoning can easily be countered by carrying out cookie clean up. As cloud computing infrastructure consists of complex layers, scholars finely chose specific components for their research. While Bhardwaj et al. (2016) emphasised on cryptography and authentication mechanisms as a means of securing the cloud, Sudha and Monica 2012; Roy et al. 2015 stipulated how to mitigate threats on the network, application and virtual machine layer. From the foregoing, these authors particularly focused on the technical issues from the providers' perspective but did not mention how to establish control measures from the third-parties and consumers' end.

More so, from the review of literatures, it is observed that ethical problems could promulgate to security issues in the practice of cloud computing. In fact, ENISA (2009) plus Zissis and Lekkas (2012) mentioned disgruntled employees as a source of security breach but did not state how to prevent disgruntling and to protect critical data from such employees. Further, ethical issues concerning how and where different cloud service providers store clients' data is an issue that worries consumers due to lose control of their data (Ratten 2012; Kerr and Teng 2012). In a nutshell, all the aforementioned literatures cited challenges, threats, vulnerabilities and countermeasures of cloud computing. While this is important, they did not postulate any ISG framework to govern the processes of establishing control measures. From the foregoing, cloud computing security issues stem from multilayer of its architecture and various attack vectors. On the other hand, while the aforementioned authors are concerned about the security issues pertaining to technical and ethical issues in cloud computing, Ko et al. (2011) mentioned that ineffective governance is the primary reason of cloud computing security issues.

Moreover, according to Van and De Haes (2018), governance in information technology practice is a new concept. This the reason many organizations have not yet imbibed in this practice. Also, some companies have the concept in place but it is not effective which is the reason for security complications in cloud computing (Rebollo et al. 2012).

Further, as attacks come in diverse ways it is pertinent that a continuous development of countermeasures, research and strategic development through governance should be encouraged. This research seeks to implement effective cloud computing security governance through corporate strategic leadership. A conceptual framework of cloud computing security governance framework is designed to align with its implementation.

## III. A CONCEPTUAL FRAMEWORK FOR THE DESIGN OF CLOUD COMPUTING SECURITY GOVERNANCE

Some researchers have developed cloud computing security governance but inclusion on implementation of security governance in cloud computing practice is lacking in their research. Although COBIT 5 framework is widely adopted for IT governance (Huygh et al. 2018). The framework consists of 37 processes and 4 management domain which is complex to implement. While the work of ISO 27001 guidelines is important, they are more of traditional IT, holistic and non-cloud computing specific. ENISA adopted ISO 27001 controls specifically focused on cloud security risk and provided guides but does not include implementation. Cloud Security Alliance focuses on identification of threats vulnerabilities and how to manage risks (CSA, 2013). Furthermore, professionals in academia and industries have not come to a consensus to adopting a specific governance framework. Hence, there is no "one-size-fit-all" in this context, to this end, organizations prefer designing their framework to fit into their busines environment (Broussard and Tero, 2007 cited by Ruben P and Miguel S 2012). Further, the framework purported in this paper, represent a conceptual framework in the design of Cloud Computing Security governance. The framework took cognizance of the governance participants within and outside the organization, contractual terms and agreements as well as information security standards and policies as depicted in figure 1. From careful consideration of literatures, the proposed framework focuses on the following areas:

1. The organization (the board of directors, executives, managers and employees)
2. Terms and agreement
3. End-user
4. Third-parties
5. Information security standard and policies

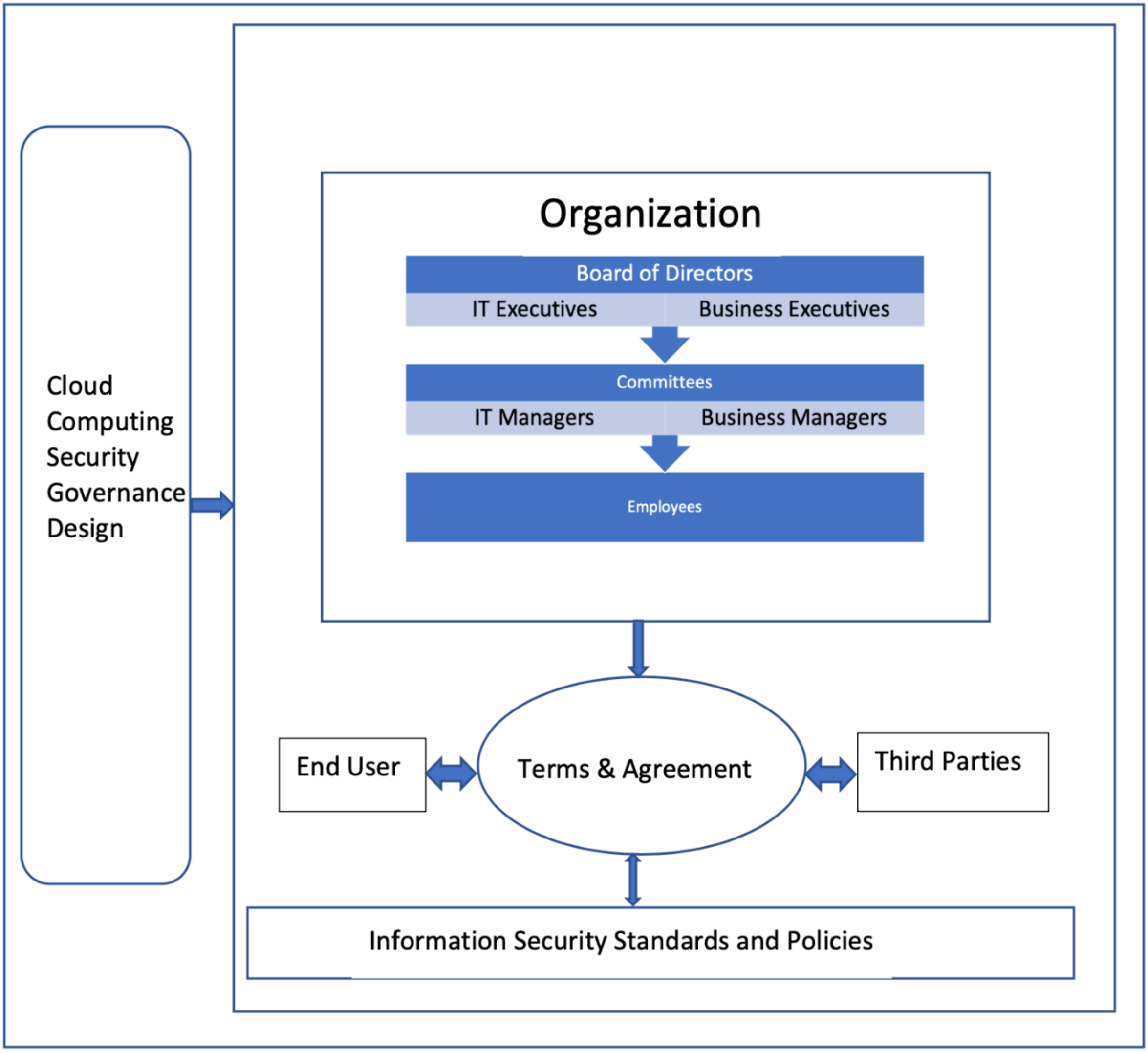


**Figure 1.** A conceptual Framework of Cloud Computing Security Governance.

## IV. EFFECTIVE IMPLEMENTATION OF CLOUD COMPUTING SECURITY GOVERNANCE

According to De Haes and Grembergen (2004) effective cloud computing security governance is the primary function of the Board of Directors (BODs) and executives. On the other hand, cloud computing security could emanate from end-users causing data loss, account hijack due to exploitation of users' credentials and loss of device (Shelveen P and Mohammed F, 2015). Therefore, while De Haes and Grembergen (2004) statement is notable, we are in agreement with a more recent opinion of Fazlida and Said (2015) stating that the appropriate tone of cloud computing security governance at the BODs level is not enough until nontechnical issues across the cloud computing community (from the top to bottom and vice versa) is tackled. Furthermore, as cloud computing practice can be seen as community, its security is a shared responsibility (Al Morsy et al. 2016). Responsibilities can be shared between the organization comprising the BODs, executives, senior management and employees, and those outside the organization which is third parties and end-users. To enhance the security of cloud computing, we identified cloud computing security governance focus areas and responsibilities of all personalities within and outside the organization as shown in table 1. However, figure 2 depicts the necessary steps taken to implement effective cloud computing security governance.

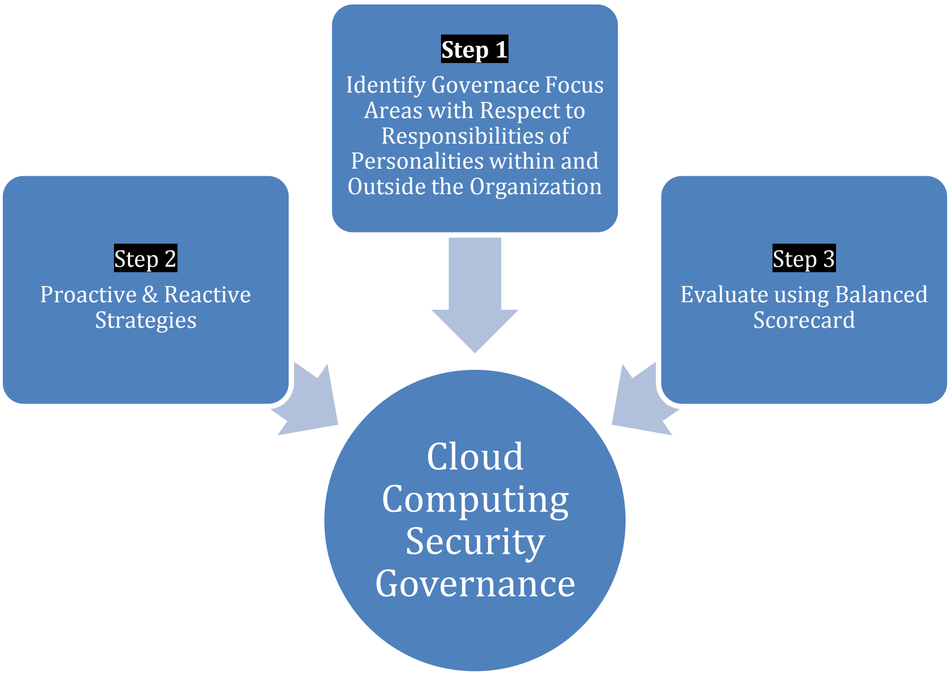
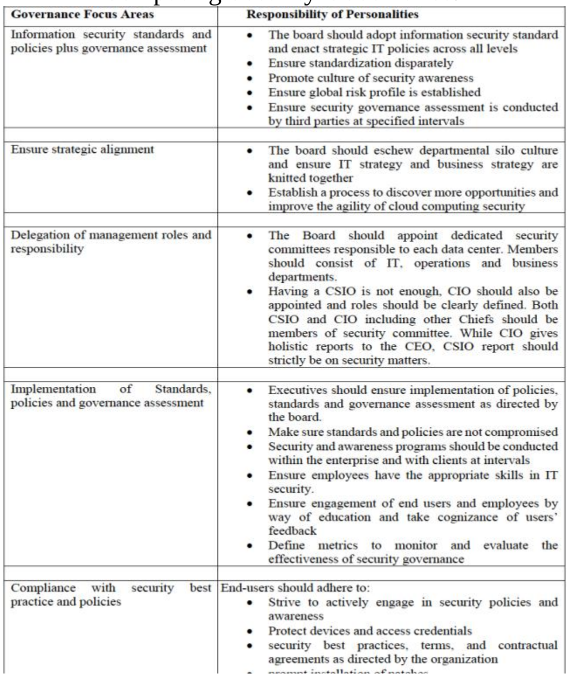

Step 1
Identify Governace Focus Areas with Respect to Responsibilities of Personalities within and Outside the Organization
Step 2
Proactive & Reactive Strategies
Step 3
Evaluate using Balanced Scorecard
Cloud Computing Security Governance

**Figure 2.** Steps to Implementing Cloud Computing Security Governance.

**Step 1: Identify Governance Focus Areas with Respect to Responsibilities of Personalities within and Outside the Organization**

Implementation of sustainable cloud computing security governance is part of corporate governance. It is chiefly the responsibility of the BODs and Executives to strategically provide direction, prioritize projects, manage risks and press towards achieving the organization's vision (De Haes and Grembergen 2004). Although implementing cloud computing security governance is a complex task. However, the complexities can be overhauled by fostering relationship between key elements: structure, processes and relational mechanism (Grembergen et al. 2004). Structures signify responsibilities of the executives, with formulation of processes, committees and also represent realistic decision-making and unceasing monitoring. Relational mechanisms include strategic alignment participation, collaboration, dialogue and education. The BODs formulate policies and are decision makers. Therefore, the manner in which policies and decisions are made can affect cloud computing security governance. Further, Rebollo et al. (2012), organizations lack effective governance resulting to discouragement in cloud computing adoption. On these notes, with reference to Figure 1, the researchers identified governance focus areas and defined responsibilities of personalities within and outside the organization as shown in Table 1.

**Table 1.** Governance Focus areas and Responsibilities of Personalities in Cloud Computing Security Governance.



| Governance Focus Areas | Responsibility of Personalities |
|---|---|
| Information security standards and policies plus governance assessment | • The board should adopt information security standard and enact strategic IT policies across all levels<br>• Ensure standardization disparately<br>• Promote culture of security awareness<br>• Ensure global risk profile is established<br>• Ensure security governance assessment is conducted by third parties at specified intervals |
| | |
| Ensure strategic alignment | • The board should eschew departmental silo culture and ensure IT strategy and business strategy are knitted together<br>• Establish a process to discover more opportunities and improve the agility of cloud computing security |
| | |
| Delegation of management roles and responsibility | • The Board should appoint dedicated security committees responsible to each data center. Members should consist of IT, operations and business departments.<br>• Having a CSIO is not enough, CIO should also be appointed and roles should be clearly defined. Both CSIO and CIO including other Chiefs should be members of security committee. While CIO gives holistic reports to the CEO, CSIO report should strictly be on security matters. |
| | |
| Implementation of Standards, policies and governance assessment | • Executives should ensure implementation of policies, standards and governance assessment as directed by the board.<br>• Make sure standards and policies are not compromised<br>• Security and awareness programs should be conducted within the enterprise and with clients at intervals<br>• Ensure employees have the appropriate skills in IT security.<br>• Ensure engagement of end users and employees by way of education and take cognizance of users' feedback<br>• Define metrics to monitor and evaluate the effectiveness of security governance |
| | |
| Compliance with security best practice and policies | End-users should adhere to:<br>• Strive to actively engage in security policies and awareness<br>• Protect devices and access credentials<br>• security best practices, terms, and contractual agreements as directed by the organization<br>• prompt installation of patches |

**Step 2: Application of Proactive and Reactive Strategies**

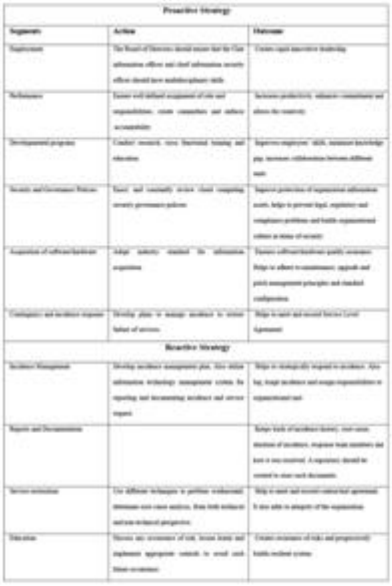
In a novel work of Souza et al. (2017),

reactive strategy comes into play when proactive strategy fails. While proactive strategy is inclined towards anticipation of risks, reactive strategy is disposed to resolving immediate risks. Often time, reactive strategies allows for review of policies (Sridhar et al. 2012). It also helps in acquisition of proactive controls and proffer continuous improvement of cloud computing security governance.

Sridhar et al. (2012) further said reactive strategy is short-term based and have finite anticipation of attacks, therefore, proactive strategy ought to be given priority over reactive strategy. That said it is incumbent on executives to research new ideas, implement, re-examine, and upgrade proactively before occurrence of risks leading to loss in the organization's business. However, the researchers are the same accord with the opinion of De Haes and Van Grembergen (2009), that effective governance is apt to strike balance of all strategies for the betterment of busines. Therefore, both strategies are important and should be given equal attention. Having effective governance structure would help to judiciously apply both strategies to improve the dexterity of cloud computing security governance.

Table2 critically present cloud computing security governance proactive and reactive strategies. It identified important segments, action to be taken and outcome respectively.

Table 2. Proactive and Reactive Strategies to implementing effective cloud computing security governance.



| Proactive Strategy | | |
|---|---|---|
| Segments | Action | Outcome |
| Employment | The Board of Directors should ensure that the Chief information officer and chief information security officer should have multidisciplinary skills | Creates rapid innovative leadership |
| Performance | Ensure well defined assignment of role and responsibilities, create committees and enforce accountability | Increases productivity, enhances commitment and allows for creativity |
| Development programs | Conduct research, cross functional training and education | Improves employees' skills, minimises knowledge gap, increases collaboration between different units |
| Security and Governance Policies | Enact and constantly review cloud computing security governance policies | Improves protection of organisational information assets, helps to prevent legal, regulatory and compliance problems and builds organisational culture in terms of security |
| Acquisition of software/hardware | Adopt industry standard for information acquisition | Ensures software/hardware quality assurance. Helps to adhere to maintenance, upgrade and patch management principles and standard configuration |
| Contingency and incident response | Develop plans to manage incidents to avoid failure of services. | Helps to meet and exceed Service Level Agreement |
| Reactive Strategy | | |
| Incident Management | Develop incident management plan. Also utilize information technology management system for reporting and documenting incidents and service request. | Helps to strategically respond to incidents. Also log, triage incidents and assign responsibilities to organisational unit. |
| Reports and Documentation | | Keeps track of incidents history, root cause, duration of incidents, response team members and how it was resolved. A repository should be created to store such documents. |
| Services restoration | Use different techniques to perform workaround, determine root cause analysis, from both technical and non-technical perspectives. | Help to meet and exceed contractual agreement. It also adds to integrity of the organisation. |
| Education | Discuss any occurrence of risk, lesson learnt and implement appropriate controls to avoid such future occurrence. | Creates awareness of risks and progressively builds resilient systems. |

**Step 3: Balanced Scorecard for monitoring and Evaluating the Cloud Computing Security Governance framework.**

It is important to continuously evaluate cloud computing security governance framework. Implementing Balanced Scorecard (BSC) to allow for alignment of cloud computing security governance strategies to the vision and mission of the organization. However, Silva and Chaix (2008) is of the opinion that evaluating this framework is complex since there is no consensus on a precise tool or technique that can be applied to know the extent to which the cloud computing security governance framework supports the security of cloud computing. Mueller et al. (2008) also affirmed that evaluation of the agility of the framework is challenging since there are different factors affecting the security of cloud computing.

Although there are different tools to evaluating the cloud computing security framework such as Process capability (PC)" presently known as "process maturity" and Return on Investment (ROI) estimation tool De Haes and Grembergen (2008). However, these tools are limited in that they can only evaluate processes and tangible assets respectively (Kwak and Ibbs 2002). Balanced Scorecard is complex to implement but it is the best tool to evaluate effectiveness of any business (Ahmad 2009). Therefore, the researchers are of the opinion that a Balanced Scorecard (BSC) should be implemented to evaluate the cloud computing security governance framework. Further, BSC is a suitable since it includes indicators and directives that give forth organizational vision. Again, it helps board members to meet stakeholders' expectations (Quesado et al. 2018) as it converts the mission and strategies into actionable steps paving way for collaboration among different functional departments, improve security, persistent feedback, learning, transparency, clear contractual terms and agreement at all levels from the organization to customers and third-parties. In this paper, we developed a BSC as shown in Figure 3. To efficiently evaluate the cloud computing security governance framework, we applied the BSC in the following areas: effectiveness of cloud computing security governance, end-users/third-parties, cloud computing security, operations, provisioning of developmental infrastructure and collaboration at all levels.

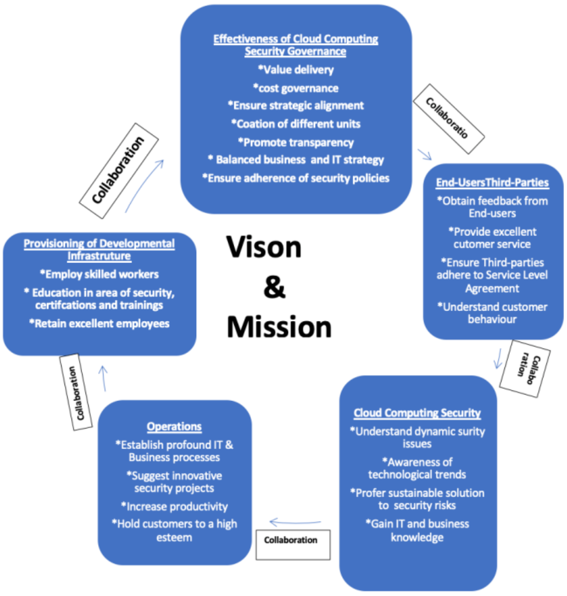

Effectiveness of Cloud Computing Security Governance
*Value delivery
*cost governance
*Ensure strategic alignment
*Coation of different units
*Promote transparency
* Balanced business and IT strategy
*Ensure adherence of security policies
Collaboratio
End-UsersThird-Parties
*Obtain feedback from End-users
*Provide excellent cutomer service
*Ensure Third-parties adhere to Service Level Agreement
*Understand customer behaviour
Collabo ration
Cloud Computing Security
*Understand dynamic surity issues
*Awareness of technological trends
*Profer sustainable solution to security risks
*Gain IT and business knowledge
Collaboration
Operations
*Establish profound IT & Business processes
*Suggest innovative security projects
*Increase productivity
*Hold customers to a high esteem
Collaboration
Provisioning of Developmental Infrastruture
*Employ skilled workers
* Education in area of security, certifcations and trainings
*Retain excellent employees
Collaboration
Vison
&
Mission

**Figure 3.** Cloud Computing Security Governance Balanced Scorecard.

## V. CONCLUSION

At the heels of insufficient literatures on cloud computing security governance, this article presents a notable contribution to pertinent research societies. Further, initial conceptual framework for the design of cloud computing security governance was presented. Roles and responsibilities from the organizational perspective, end-users third-parties, information security governance and policies plus terms and agreement were identified. Furthermore, three important steps were discussed to implement effective cloud computing security governance. However, future work needs to be done to capture more holistic steps to implementing cloud computing security governance.

In this paper, it is also stated there is no unanimous cloud computing security governance framework, hence it is not appropriate to generalize the implementation steps as organizations differs in requirements as well as challenges. Therefore, any organization that intend to implement cloud computing security governance should regard the implementation steps as guidelines as this has to be tested and validated through empirical studies. Future work will validate the implementation steps in a real-life case study with structured methodology.

## REFERENCES

[1]. Ahmad, M. I. (2009). IT BSC: a comprehensive framework for IT evaluation, IT management, and IT governance. nature, 5, 6.

[2]. Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107. https://www.cs.auckland.ac.nz/~john-g/papers/cloud2010_1.pdf

[3]. Ashktorab, V., &Taghizadeh, S. R. (2012). Security threats and countermeasures in cloud computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 1(2), 234-245.

[4]. Bhardwaj, A., Subramanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Review of solutions for securing end user data over cloud applications. International Journal of Advanced Computer Research, 6(27), 222.

[5]. Cloud Security Alliance – CSA, Top Threats Working Group (2013). The Notorious Nine - Cloud Computing Top Threatsin 2013. http://www.cloudsecurityalliance.org/topthreats.

[6]. Cloud Security Alliance – CSA (2011). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. http://www.cloudsecurityalliance.org/guidance/

[7]. De Haes, S. and Van Grembergen, W., 2009. An exploratory study into IT governance implementations and its impact on business/IT alignment. Information Systems Management, 26(2), pp.123-137.

[8]. De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. Information systems control journal, 1, 27-33.

[9]. Devi, M., Saini, M. S., & Pandey, M. C. Security and Privacy Concerns in Cloud Computing.

[10]. European Network and Information Security Agency – ENISA (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment/at_download/fullReport

[11]. Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. Procedia Economics and Finance, 28, 243-248.

Hussein, N. H., & Khalid, A. (2016). A survey of cloud computing security challenges and solutions. International Journal of Computer Science and

Information Security, 14(1), 52.

[12]. Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. (2018, January). Answering key global IT management concerns through IT governance and management processes: A COBIT 5 View. In Proceedings of the 51st Hawaii International Conference on System Sciences.

[13]. Kwak, Y. H., &Ibbs, C. W. (2002). Project management process maturity (PM) 2 model. Journal of management in engineering, 18(3), 150-155.

[14]. Lu, J. (2019). Assessing The Cost, Legal Fallout Of Capital One Data Breach. Legal Fallout Of Capital One Data Breach (August 15, 2019).Shelveen Pandey, MohammedFarik http://www.ijstr.org/final-print/nov2015/Cloud-Computing-Security-Latest-Issues-Countermeasures.pdf

[15]. Mishra, A., Mathur, R., Jain, S., & Rathore, J. S. (2013). Cloud computing security. International Journal on Recent and Innovation Trends in Computing and Communication, 1(1), 36-39.

[16]. Mueller, L., Magee M., Marounek, P., and Phillipson A., 2008. IBM IT Governance Approach Business Performance through ITExecution. http://www.redbooks.ibm.com/redbooks/pdfs/sg247517.pdf

[17]. Pereira, R., & da Silva, M. M. (2012). IT governance implementation: The determinant factors. Communications ofthe IBIMA, 2012, 1.

[18]. Quesado, P. R., Aibar Guzmán, B., & Lima Rodrigues, L. (2018). Advantages and contributions in the balanced scorecard implementation. Intangible capital, 14(1), 186-201.

[19]. Ratten, V., 2012. Entrepreneurial and ethical adoption behaviour of cloud computing. The Journal of High Technology Management Research [online], 23(2), 155-164.

[20]. Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. J. UCS, 18(6), 798-815.

[21]. Roy, A., Sarkar, S., Ganesan, R., & Goel, G. (2015). Secure the cloud: From the perspective of a service-oriented organization. ACM Computing Surveys (CSUR), 47(3), 1-30.

[22]. Silva, E., &Chaix, Y. (2008, January). Business and IT governance alignment simulation essay on a business process and IT service model. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 434-434). IEEE.

[23]. Simonsson, M., Johnson, P., &Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. Informationsystems management, 27(1), 10-24.

[24]. Souza, V. B., Masip-Bruin, X., Marín-Tordera, E., Ramírez, W., & Sánchez-López, S. (2017, June). Proactive vs reactive failure recovery assessment in combined Fog-to-Cloud (F2C) systems. In 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-5). IEEE.

[25]. Sperling, J., & Webber, M. (2019). The European Union: security governance and collective securitisation. West European Politics, 42(2), 228-260.

[26]. Sridhar, S., Hahn, A., &Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 100(1), 210-224.

[27]. Sudha, M., & Monica, M. (2012). Enhanced security framework to ensure data security in cloud computing using cryptography. Advances in Computer Science and its Applications, 1(1), 32-37.

[28]. Torkura, K. A., Sukmana, M. I., Cheng, F., &Meinel, C. (2019, September). Security chaos engineering for cloud services: Work in progress. In 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA) (pp. 1-3). IEEE.

[29]. Van Grembergen, W., & De Haes, S. (2018, January). Introduction to the Minitrack on IT Governance and its Mechanisms. In Proceedings of the 51st Hawaii International Conference on System Sciences.

[30]. Zissis, D., &Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation computer systems, 28(3), 583-592.