Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.48 – 56

RESEARCH ARTICLE

Information System Audit: Cloud Computing Security and Challenges

Abhijit Gupta[1], Subarna Shakya[2]

[1]School of Computer Science and IT, Singhania University, India

[2]Department of Electronics and Computer Engineering, Institute of Engineering, Tribhuvan University, Nepal

[1] abhi@abhi.com.np; [2] drss@ioe.edu.np

Abstract—The Cloud Computing paradigm is getting popular deliberately and is being adopted in modern organizations because of its lower cost, scalability and high availability. This moves control of data from the owner to the cloud service provider and thus security and data privacy of customer or owner becomes a challenge. Cloud is a new concept and as a result of which the experience of providers in this field might not be enough to complement security. Security, being inconsistent and not robust, will have low credibility on the benefit that features of cloud computing has to offer. This research is done using exploratory method and presents an explanatory review on Information System (IS) Audit on cloud computing and security issues and prescribes a framework that can be used for Cloud Computing and Security. This research proposes an audit model for cloud computing.

Keywords— Information System Audit, Cloud Computing, Security, Information System, Cloud reliability and performance

I. INTRODUCTION

With growing dependency on internet for globalization, cost for owning IT Infrastructure, resources have increased. Cloud computing is a new concept that usually is an on demand leasing service for internet applications and IT resources. According to NIST definition, "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". [1]

Cloud computing reduces huge upfront investments and recurring ongoing maintenance cost due to its principle of "pay for what you use" [2]. In cloud computing, the resources can be in someone else's premises or network commonly known as providers. The resources can be leased and are accessed remotely by cloud users or cloud service buyers via internet or network. All request received by the cloud servers are processed and the output is sent back as normal process [3].

The cloud computing gives three sensitive states of concern in operational context of cloud

- Sending of data to the cloud,
- Receiving of data from the cloud to clients computer,
- Storage of data in remote cloud server which client may or may not own.[5]

Cloud computing has several advantages but at the same time it opens up risks on security issues. The remote access could lead to security threats for which Information System (IS) Audit can be helpful.

The research has been conducted with a study on Essential Characteristics, Service and Deployment Models of Cloud Computing. Next section of this paper shows security issues in the cloud computing and discussion on authentication of cloud computing.

II. OBJECTIVE

The main objective of this research is to study security and challenges in cloud computing and propose a model for IS audit for cloud computing.

III.LITERATURE REVIEW

A. Cloud Computing

The concept of cloud computing has evolved from grid computing. The meaning of cloud computing can be generalized as the features and services where the computing is done at own or third-party's network and the ownership of the IT infrastructure may be with self or external [4, 5].

Cloud computing shows five essential characteristics that separate it from typical computing processes such as

- On-demand self-service: It provides unilateral provision to cloud service buyer for computing without requiring human interaction with service provider.
- Broad network access: It provides heterogeneous client platform (such as laptops, smart phones) to access the cloud.
- Resource pooling: It provides pooling resources to multiple consumers and the resources can be assigned by cloud dynamically and reassigned as per the demand.
- Rapid elasticity: The provisions of capabilities could be rapidly scaled in or out as needed.
- Measured Service: It provides metering capability to monitor, control and create reports for resource usages.

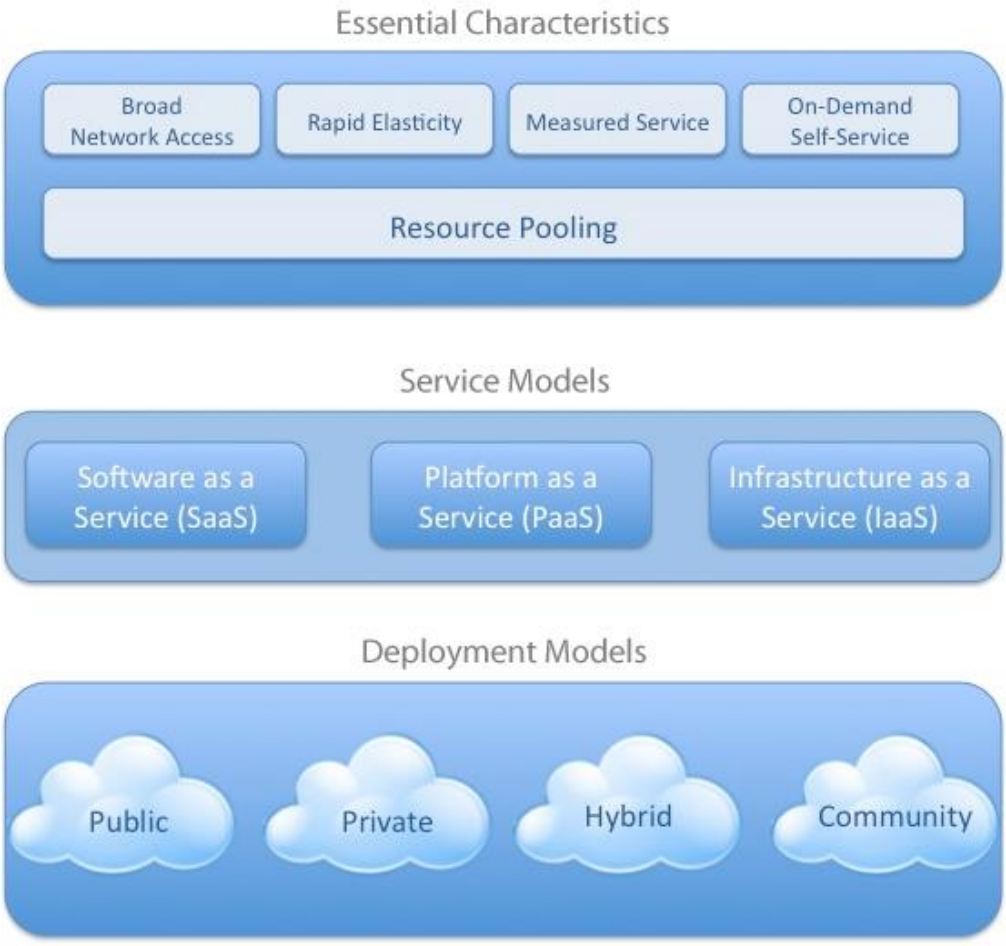

Fig. 1. Visual Model of NIST Working Definition of Cloud Computing [6]

Cloud services are delivered using three archetypal models and several derivation combinations. The three delivery models of cloud are

- Software as a Service (SaaS): In SaaS delivery model, cloud service buyer is not required to manage the infrastructure. However, they are provided with a client panel from where they can manage their applications across different platforms.
- Platform as a Service (PaaS): In PaaS model, cloud service buyer can deploy self-created, owned or acquired applications. Here, buyers are not required to manage to infrastructure, OS or storage.
- Infrastructure as a Service (IaaS): In IaaS model, cloud service buyer has controls over deployed applications, OS, storage and possibly limited select networking control. [6, 7]

Cloud computing solution offers four types of cloud deployment models such as

- Public Cloud: It is owned by cloud service provider but made available to any general user or public or large industry.
- Private Cloud: It can be on-premises or off-premises and owned by single organization and managed self or get managed via third-party provider as required.
- Community Cloud: It can be on-premises or off premises and is shared by numerous organizations to support a specific community for a Compliance consideration, policy, security requirements, mission, or any shared concerns.
- Hybrid Cloud: It is combination two or more of above clouds that is private community or public. [6,7,8]

The context for cloud deployment and usage modalities is not just internal or external physical locations. The context is the user and expert responsible for its security, governance and compliance. Fig.2 depicts different cloud computing deployment models.

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization / Third Party Provider	Organization / Third Party Provider	On-Premise / Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

[1] *Management includes: governance, operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual/ policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

Fig. 2. Cloud Computing Deployment Model [6]

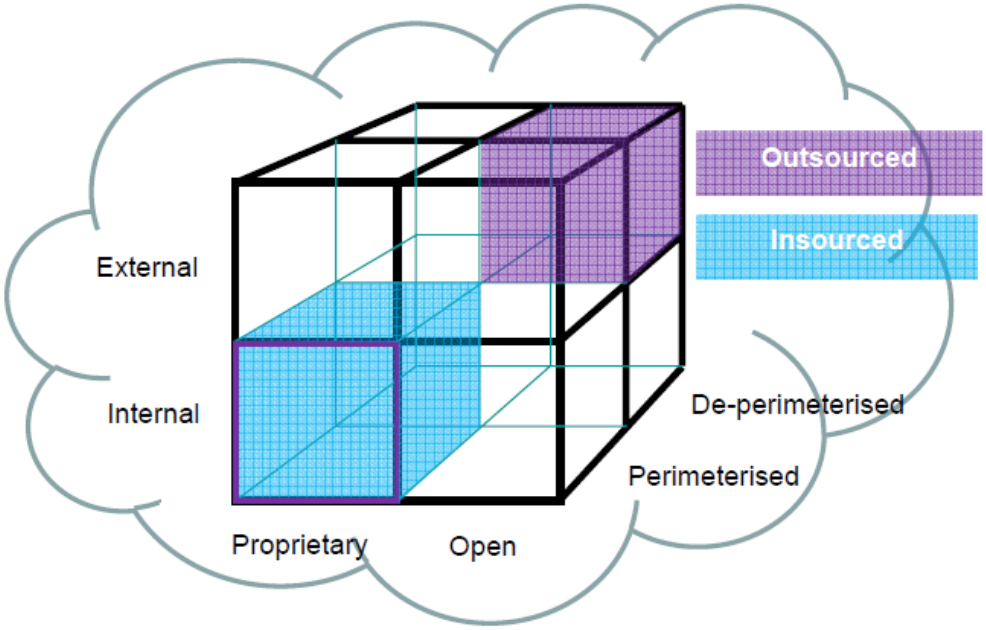

Fig. 3. Jericho Cloud Cube Model [9]

There is an another way to visualize the combination of deployment model, cloud service model, physical resource location and attribution of management and ownership known as Jericho Cloud Cube Model as shown in Fig.3. which provides many permutations of cloud offerings today. [9]

A survey undertaken by International Data Corporation (IDC), according to the majority of results (Fig.3), shows that cloud computing is the most low cost viable option for users as shown in the Fig. 1 below. The three options on top five such as "pay only for what you use, monthly payments and requires less in-house IT staff, costs" were perceived for the cost benefit of the cloud model. The result also showed that cloud computing is suitable for such people or startup looking for quick, cheap and reliable solution such as developers, researchers or ecommerce solution providers. [10]

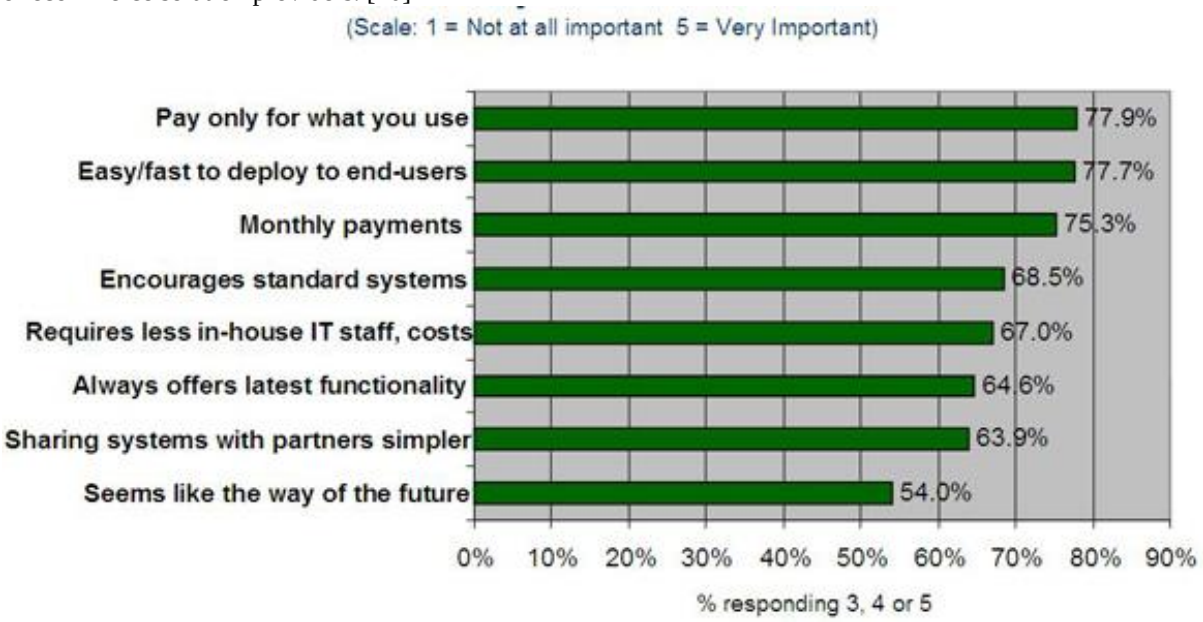

Fig. 4. Benefits commonly ascribed to the 'cloud'/ on-demand model [10]

B. Security and Challenges

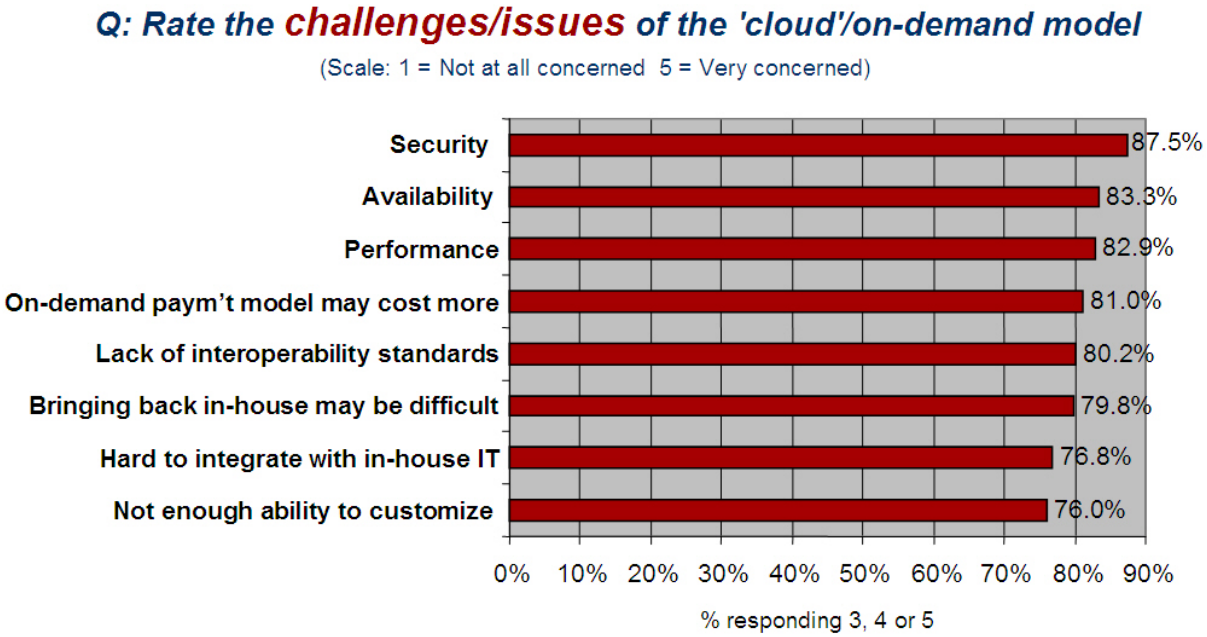

Fig. 5. Challenges/Issues of the cloud/on-demand model [10]

A survey conducted by IDC, according to majority of results as shown in Fig.4.), shows that for a provider, security is the prime concern in cloud to tackle with in order to maintain their position as market leaders. Similarly, Availability and Performance, together also can be labelled as Dependability, is second bigger challenge in the cloud [10].

Fig. 6 depicts comparison of cloud service mapping against compensating controls to check existence of controls. It can be compared to compliance framework or PCI DSS as shown in Fig.6. This gap analysis helps to determine steps for risk assessment framework which determines how gaps and risks should be accepted or transferred or mitigated.

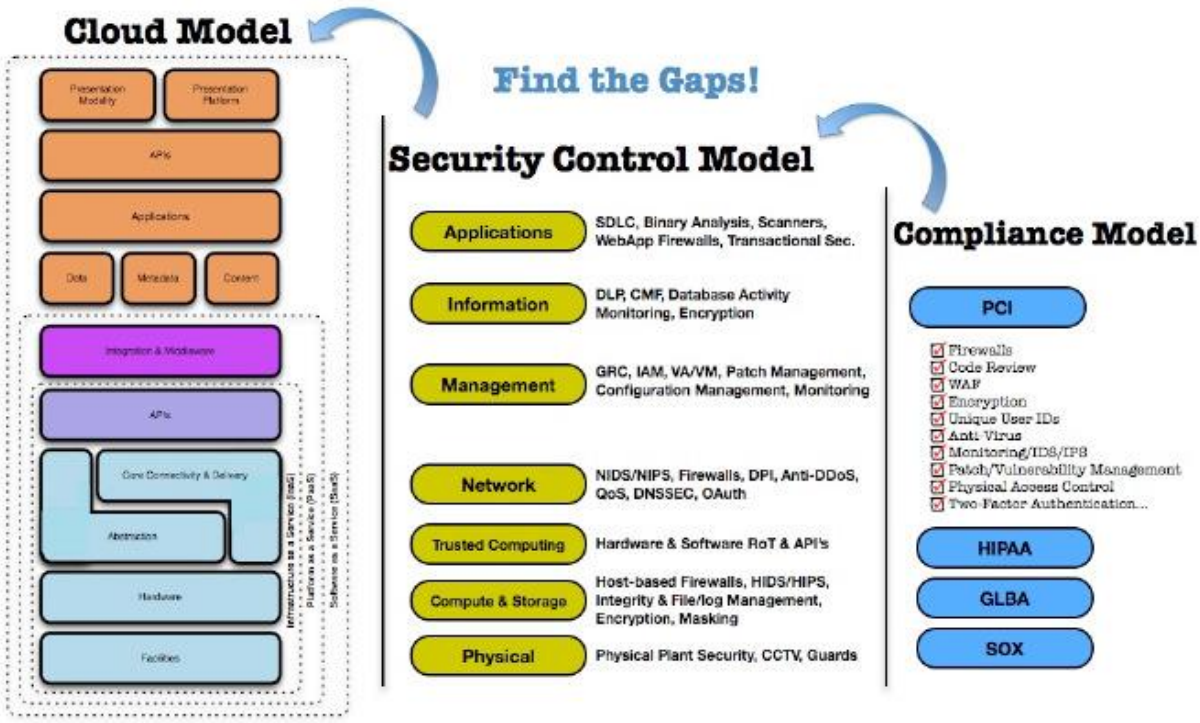

Fig. 6. Mapping the Cloud Model to the Security Control & Compliance Model [6]

Before addressing anything more about the security audit on cloud, it is important to question what part of IT should be moved to the cloud. This helps figuring security challenges in internal IT before facing security concerns while adopting cloud computing. However, Internal IT is security is not very easy to attain because

- The availability of skilled security professional is low.
- Good security costs more money.
- Security and IT staff might have interest in the contents of the data.
- Any human resource having access to the data center has access to data.
- Most internal IT organization and business grew together.

The cloud computing has both internal and external threats like any internal IT that can be accepted or mitigated as shown in the Table I. [11]

TABLE I
MINI CLOUD RISK/ MITIGATION TABLE [11]

Risk	**Mitigation**
Multi-tenancy	Infrastructure/data segregation
Ever developing risk	Continuing risk assessment program, CSO/CISO, Assessment
Relaxation of security	Periodic assessment/audit
Service provider tiers	Contract pass-through, coordinated security assessment
Contractor access	Background checks, Contracts, Segregation, Surveillance
Disasters	SLA, Multi facility provisioning
External Physical	Secure facility, Escort, Surveillance
External Logical	IPS, Firewalls, WAF, Secure Coding, Secure Architecture, Host hardening
Incidents	Facility & Per Customer Incident Response Plan
Application bugs	Layered security, Patching, Secure coding practices, Assessments, Segregation
Data leakage	Encryption (at rest & in flight), Segregation, Assessment, Host hardening

C. Information System Audit

Information System Audit is a process of assessing risks so that its security can be enhanced [12]. Audits are independent assessment which could also provide gap analysis on the internal controls effectiveness of an IS [13].

International Organization for standardization has defined

- ISO27000 series is on IS Security and ISO27008 for Information and Security Management Auditing that focuses on ISMS latter rather than specific controls. [12]
- ISO31000 for risk management
- ISO/IEC27033-1 as the concept of network security that provides necessary guidance on its management [12, 14].
- ISO17799:2005 as specification of audit process for information system security assurance. [15]
- ISO19011:2003 as flow of management of Audit program. [16]

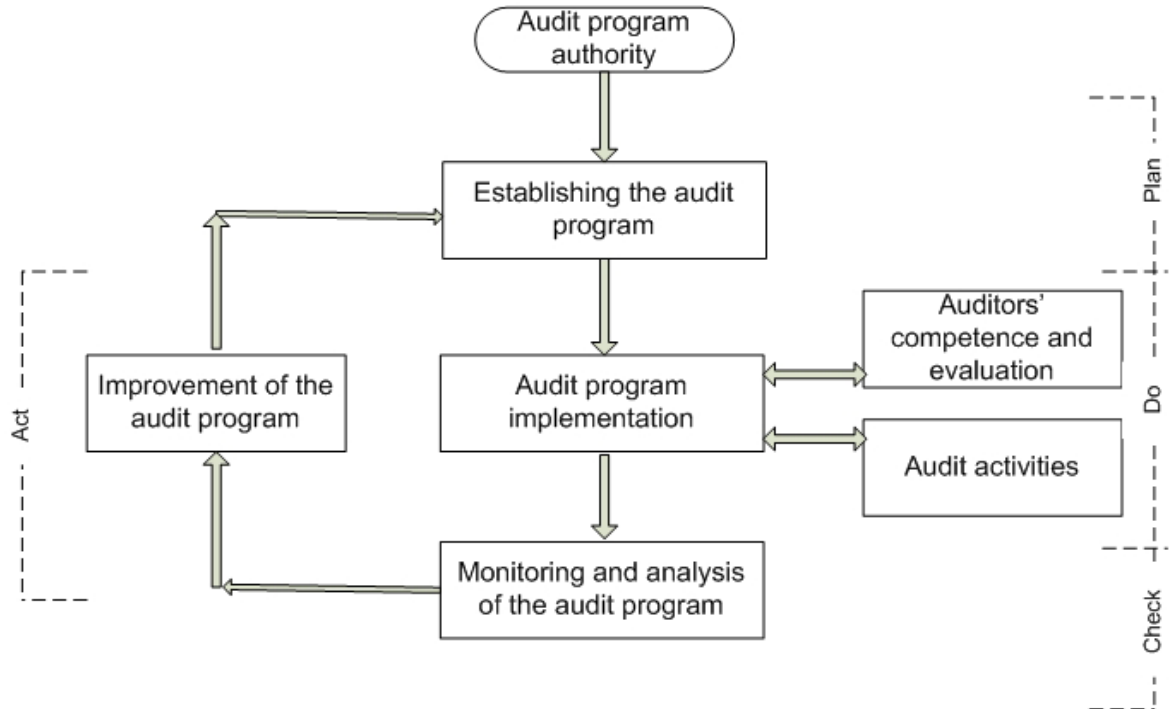

Fig. 7. Audit Program Management process flow [16]

Audit program can be established upon identifying purpose and scope of audit program, responsibilities of an auditor, resources supporting audit program and procedures that specify operations to be followed to reach the goal as shown in Fig.7. Audit program can be implemented upon audit programming, auditor's evaluation, audit team selection, audit activity management and record maintenance. Audit can be monitored and analysed to identify the preventive and corrective actions and improvement opportunities. Audit program closely follows "Deming Cycle: Plan-Do-Check-Act (PDCA)" as shown in Fig.7.

IV. RESEARCH METHODOLOGY

This research uses explanatory method and has been conducted by observing phenomena, behaviours or problems to seek answers on how audit on cloud computing can be conducted. The data for this research has been collected through published research papers and articles. [17]

V. RESULTS, ANALYSIS AND DISCUSSION

The audit model as in Fig.8 for cloud computing has been proposed by researcher where the audit has been broken into three major sections – Study, Assessment, Corrective Actions and Recommendations. The study section is for the auditors where they need to prepare themselves by learning Organizations Security and ICT policy, Legal compliances, Cloud Deployment Model and architecture, Communication and Operational policy and standards. This gets auditor to shape themselves with respect to organizations working culture and thus assessment of risk becomes effective. The assessment can be done at least for four major domains such as Security, Availability, Performance and Compliance. There are several tools to exhibit that, such as, vulnerability scanner, network protocol analyzer, intrusion detection systems, wireless sniffers, web scanners, email server scanners, virus scanners etc. These help in producing reports for corrective actions and recommendations which can be discussed with the stake holders and final audit reports can be prepared.

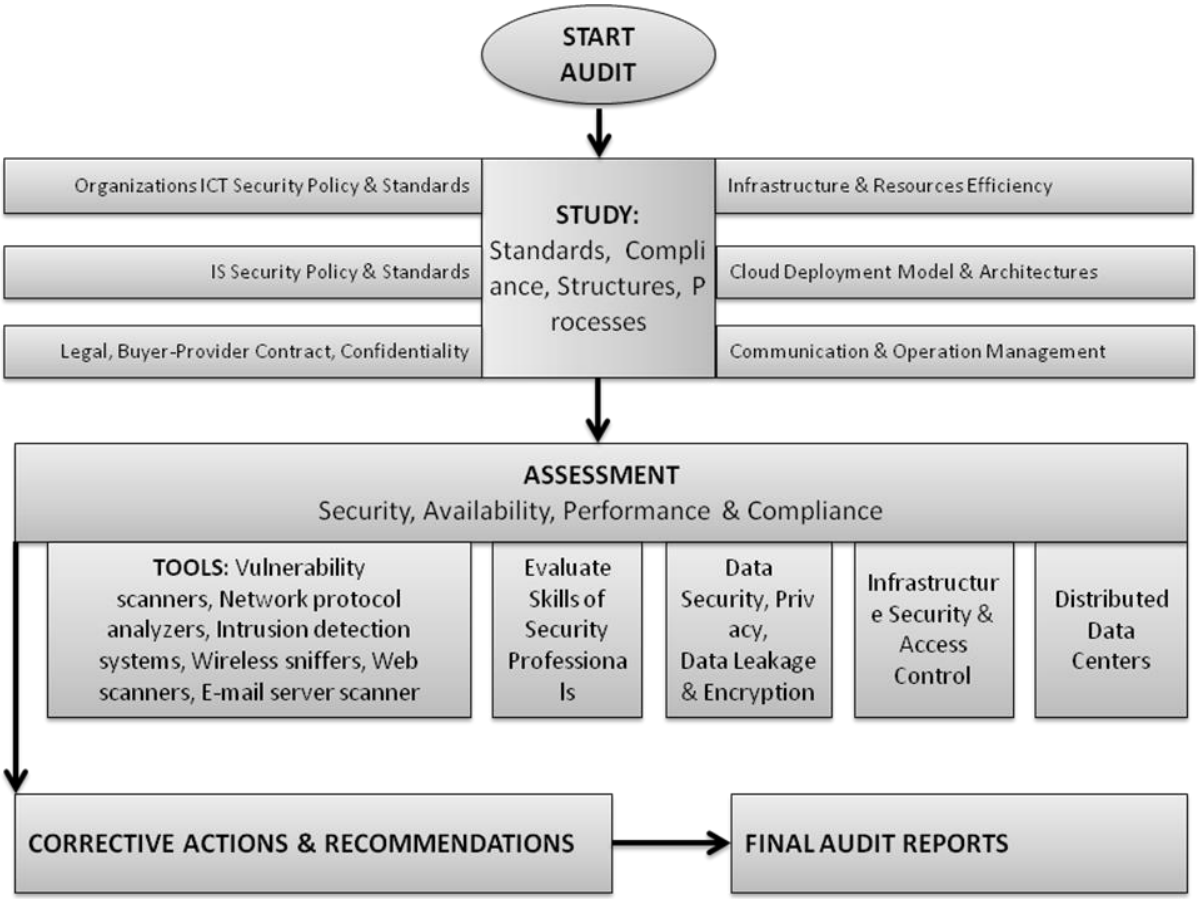

Fig. 8. Cloud Computing Audit Framework

VI. CONCLUSION

Cloud computing is faster, cheaper and easiest means of solutions for computing. Risk assessment and security audit has to be conducted eventually to minimize and mitigate risks. Local law, Local and International standards and policy must be followed while preparing the ICT Security policies in an organization. Audit is must for data security assurance. This research has proposed an audit model for cloud computing which is highly recommended for IS Audit in cloud computing and security vulnerability minimizing.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude towards my family for their kind help and support. I would like to thank my Supervisor Prof. Dr. Subarna Shakya for his kind support and help on this research. I would like to thank other research scholars in my university such as Mr. Rajendra Man Banepali, Mr. Shreedhar Marasini and Mr. Mahesh Maharjan for their valuable input and assistance on my research.

Furthermore, I would like to thank all those respondents who participated in my online survey and helped me in the data collection. Last but not least, I would like to thank you all who has gone through my paper and I would appreciate if you can give me your feedback on this.

REFERENCES

[1] P. Mell, T. Grance, "The NIST definition of Cloud Computing", September 2011.

[2] Amazon Web Services, "What is cloud computing?", http://aws.amazon.com/what-is-cloud-computing/, November 2015

[3] Petre, R., "Data mining in Cloud Computing". Database Systems Journal, 3(3), 67-71, 2012

[4] J. Che, Y. Duan, T. Zhang, and J. Fan, "Study on the security models and strategies of cloud computing", Procedia Engineering, 23, 586 – 593, November 2011.

[5] M. Ahmed and M. A. Hussain, "Cloud Computing and Security Issues in the Cloud", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[6] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1", Decebmber 2009

[7] S. Ramgovind, MM. Eloff, E. Smith, "The Management of Security in Cloud Computing", 978-1-4244-5495-2/10/$26.00 © 2010 IEEE

[8] D. Jamil and H. Zaki, "Security Issues in Cloud Computing and Countermeasures", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4, April 2011.

[9] Jericho Forum, "Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", V1.0, April 2009, http://www.opengroup.org/ jericho/cloud_cube_model_v1.0.pdf, Accessed 31 Nov 2015.

[10] F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, http://blogs.idc.com/ie/?p=730, 2009.

[11] C. Almond, "A Practical Guide to Cloud Computing Security", From Accenture & Microsoft, August 2009.

[12] A. Gupta, S. Shakya, "Information System Audit; A study for security and challenges", 2015, International Journal for Computer Science and Information Security, IJCSIS November 2015 Volume 13, No. 11.

[13] A. Gupta, S. Shakya, "Information System Audit; An Overview Study in E-Government of Nepal", International Conference on Green Computing and Internet of Things, 2015.

[14] ISO, "The ISO 27000 Directory", Retrieved October 2015, from http://www.27000.org/

[15] ISO, "ISO/IEC 17799:2005", Retrieved October 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=39612

[16] M. Popa and C. Toma, "Stages for the development of the Audit processess of Distributed Informatics Systems", Journal of Applied Quantitative Methods, Vol.4.No.3, 2009.

[17] A. Bhattacherjee, "Social Science Research: Principles, Methods, and Practices", USF Open Access Textbooks Collection, Book 3, Pp 6, 2012.

