Cloud Computing Security Framework for Banking Industry

Meskerem Alemu
emamenate@yahoo.com

Abrehet Mohammed Omer
Addis Ababa Science and Technology University, Ethiopia
abrehet@gmail.com

Abstract

Cloud computing is a prospering technology that most financial organizations are considering for adoption as a cost effective strategy for managing Information Technology (IT). However, financial organizations such as banks still consider the technology to be associated with many business risks that are not yet resolved. Such issues include security, privacy, legal, compliance and regulatory risks. As an initiative to address such risks, cloud security framework and bank enterprise framework have been proposed. However, the proposed framework focuses more on technical control and doesn't incorporate the overall administrative, legal and compliance control on cloud computing services. Further they are not also considered specific solutions for the bank industry compliance requirement and neglect some major bank information security issues. Due to lack of professionals and adequate frameworks in the area, the issue is getting scaled up to become a severe problem. The main objective of this paper is, therefore, to propose Cloud Computing Security Framework for the banking industry.

The study has been conducted on Banking Industry through systematic literature review on cloud computing standards, policy and best practices coupled with interview as methods of data collection. The survey result helps for identifying professionals thought on the subject and major pillars to propose new framework. Besides, the Sherwood Applied Business Security Architecture (SABSA) framework was used as a guide for designing the newly proposed cloud computing security framework for the banking industry focusing on architects view from six perspectives.

The proposed framework aggregates different temples: Risk Matrix Template, Control Domain Template, Compliance Matrix Template, and Security Strategy/Major, that help banks come up to solutions for measuring risk, compliance and setting suitable security major.

Keywords: Cloud computing; Banking industry; Metrics; Security; Threats; Vulnerability

1. Introduction

In order to satisfy customer need, banks use Information Technology (IT) services. However, traditional IT computing technology until now, has typically been a costly hurdle for financial institutions, particularly those in emerging markets where developing customized solutions or investing in advanced banking platforms has either been unfeasible or the result has seen too many failures, too many resources used and too much time wasted [1, 2].

Currently, cloud computing technology has brought the idea of storing and managing data on virtualized servers so that, applications, individuals and organizations around the world can have the ability to connect to data and computing resources anywhere and anytime. However, banks cannot afford the risk of a security breach since security of financial, personal data and mission-critical applications are paramount. Moreover, financial compliance regulations require that, data should not be intermixed with other data types, on shared servers or databases. Therefore, to move banks into cloud computing environment it is essential that security challenges in relation to regulatory policy, compliance and standards must be addressed primarily.

This research attempts to answer the research question:

What are the suitable security components to propose new Security Framework for the banking industry to adopt cloud computing services?

2. Related Work

Temenos Enterprise Framework Architecture (TEFA) (see Figure 1): The framework is focused in providing information to implement evolving product and service portfolios without disrupting banking operations [3]. In the framework, Security Management System (SMS) is incorporated as one component. The framework addresses one security domain issue, that is, identities and accesses management level. Since, cloud computing related to banking services is a broad concept other security related to administrative, technical and physical control should be addressed in broad manner.

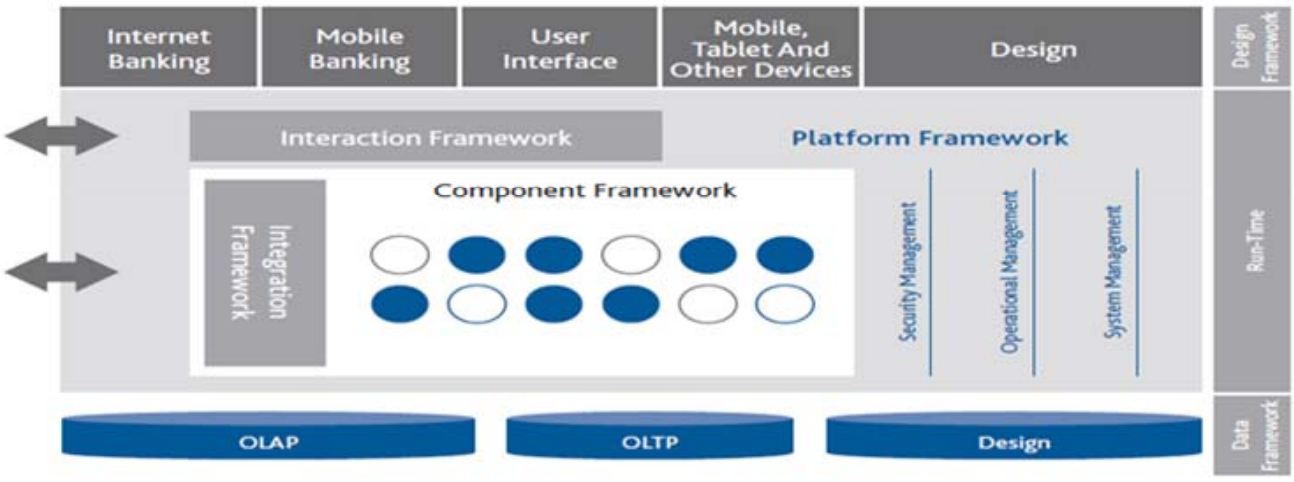

Figure 1: Temenos Enterprise Framework Architecture

IBM Security Overview on Cloud computing: in viewing of security in cloud computing, IBM proposed Security Framework (see Figure 2) [4]. IBM security framework is composed of five main components: people and identity, data and information, application and process, network, server, end point and physical infrastructure. IBM framework identifies main component in general. However, the framework is not designed basing cloud computing architecture and banking business security requirements. It doesn't address the security majors that should be considered at each level of cloud services model (i.e., SaaS, PaaS, IaaS) and deployment mode. In addition to this, regulation standards and compliances and the way to adopt cloud computing for banking services is not addressed in the framework [5].

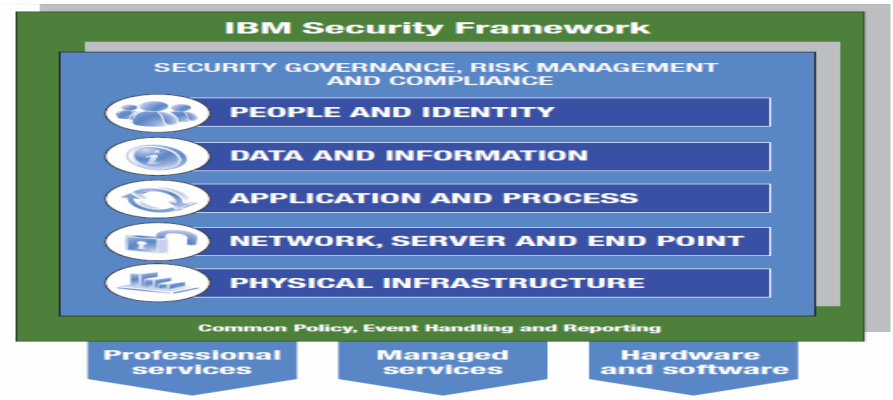

Figure 2: IBM Security Framework

In a paper "Security Issues of Banking Adopting the Application of Cloud Computing", the authors stated that, cloud technology makes possible to reuse IT resources for banks very efficiently. In order for banks to adopt this technology the paper states that two primary challenges, namely, security and regulatory compliance should be addressed, wherein financial institutions must select the right service, deployment, and operating models to address security and compliance concerns. The paper discusses security risk on cloud which includes, regulatory compliance, data location, data segregation, recovery investigation support and long term liability, leakage of data, database and server security for the system. The paper suggests that banks to use hybrid cloud since it would have private cloud for highly secured transaction [6].

In view of the advantages of cloud computing, the working group, Reserve Bank of India analyzes and recommends the support of non-financial services to ideally explore cloud computing as to gain more experience. The working group recommends that there is need of more research and development in the area of cloud governance and audit, cloud management and cloud securing technology for which the banking industry and the software industry could take the initiative so that regulatory authorities can make use of the same security framework standards [7, 8].

As different security standards and enterprise security architecture guidance provider indicates security framework shall provide much more to the business requirements than pure "security and control" [9, 10, 11, 12]. They propose enterprise security framework to address the entire three security control domain Technical, Administrative and Physical /environmental control.

Based on these facts we can say that previous works on security framework do not cover the overall security issues on cloud architecture and banking business operation.

Therefore, this paper addresses this gap by developing security framework considering banking business security requirements and cloud computing technical, physical and administrative control requirements.

3. The Proposed Framework

In order to come up with integrated security framework solution, through adopting enterprise security architecture tool of Sherwood Applied Business Security Architecture (SABSA) of architects view, we designed a cloud computing security framework for the banking industry (see Figure 3).

Cloud Model - (What and Who)

In the proposed framework of Figure 3, the system that needs to be secured in cloud system is represented with cloud architecture with main security item components such as Physical, Network, Compute, Storage, Application and Data. Cloud Services Model (SaaS, PaaS and IaaS) and Cloud Deployment Model (public, hybrid, community and private) are also integrated into the Cloud model as they are main parts of cloud architecture. For answering *who*, cloud actor is specified within cloud model. Specific actors are identified which are, bank (cloud consumer) and cloud services provider (CSP).

Security Model-(Why and Where)

Security model layers of the framework are defined with two security solutions package, Risk Matrix for answering *why* and Control Domain for answering *where*.

Risk assessment needs to occur before an enterprise enters into a cloud computing arrangement to help avoid surprises and minimize the costs of implementing and maintaining controls. More so, implementing too many controls may not be the best risk-mitigation approach, because the benefit from implementing controls should outweigh the cost. Therefore, other risk-mitigation measures such as transferring, avoiding or accepting the risk are worth considering as well. In order to address this issue through following ISO 3100 risk management guideline, we developed Risk Exposure Majoring Template (see Figure 4).

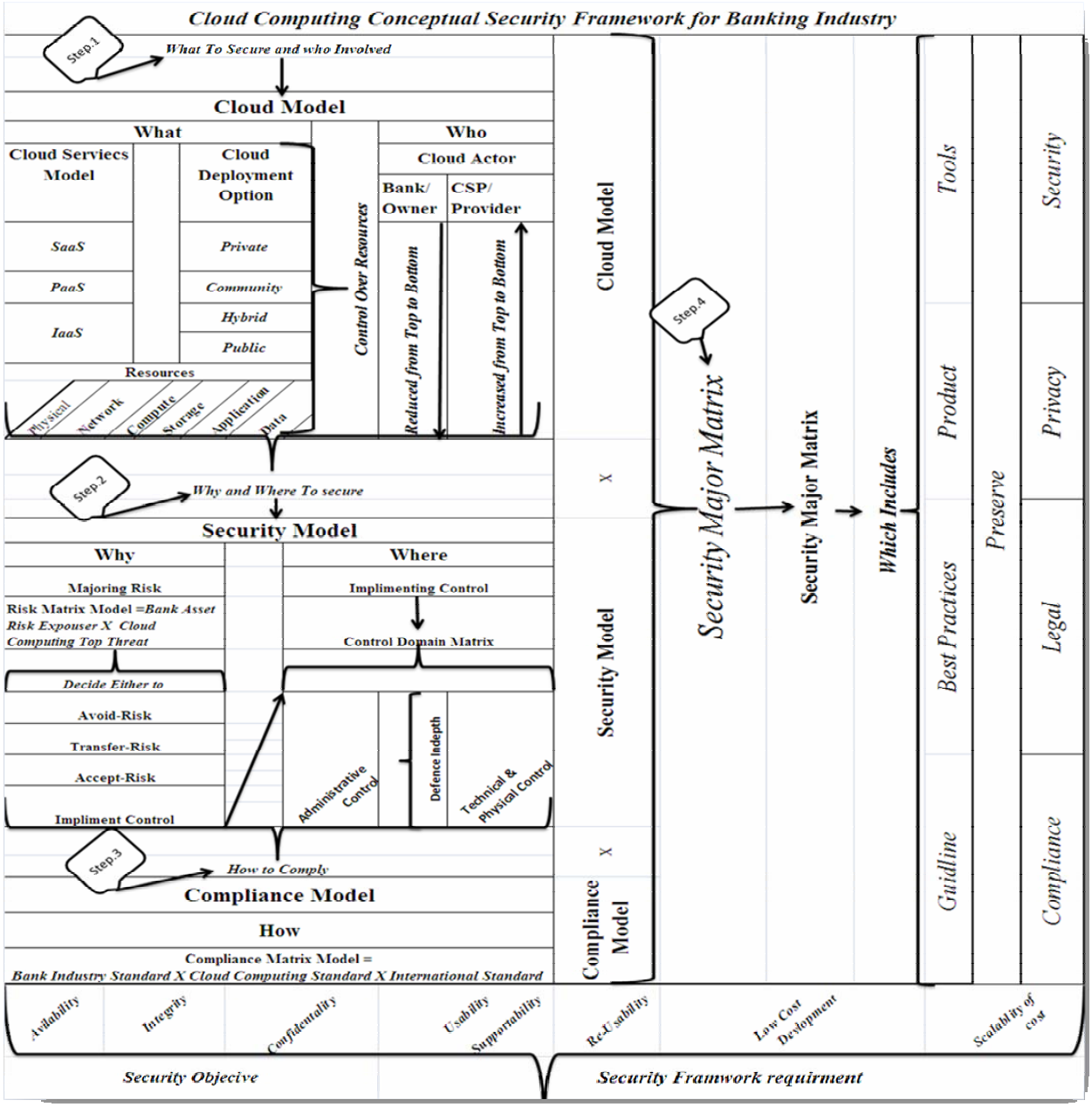

Figure 3: The Proposed Cloud computing Security Framework for Banking Industry

It is a tool for identifying banking business risk exposure through majoring risk impact and likelihood of risk exposure in deploying bank asset in each cloud deployment model.

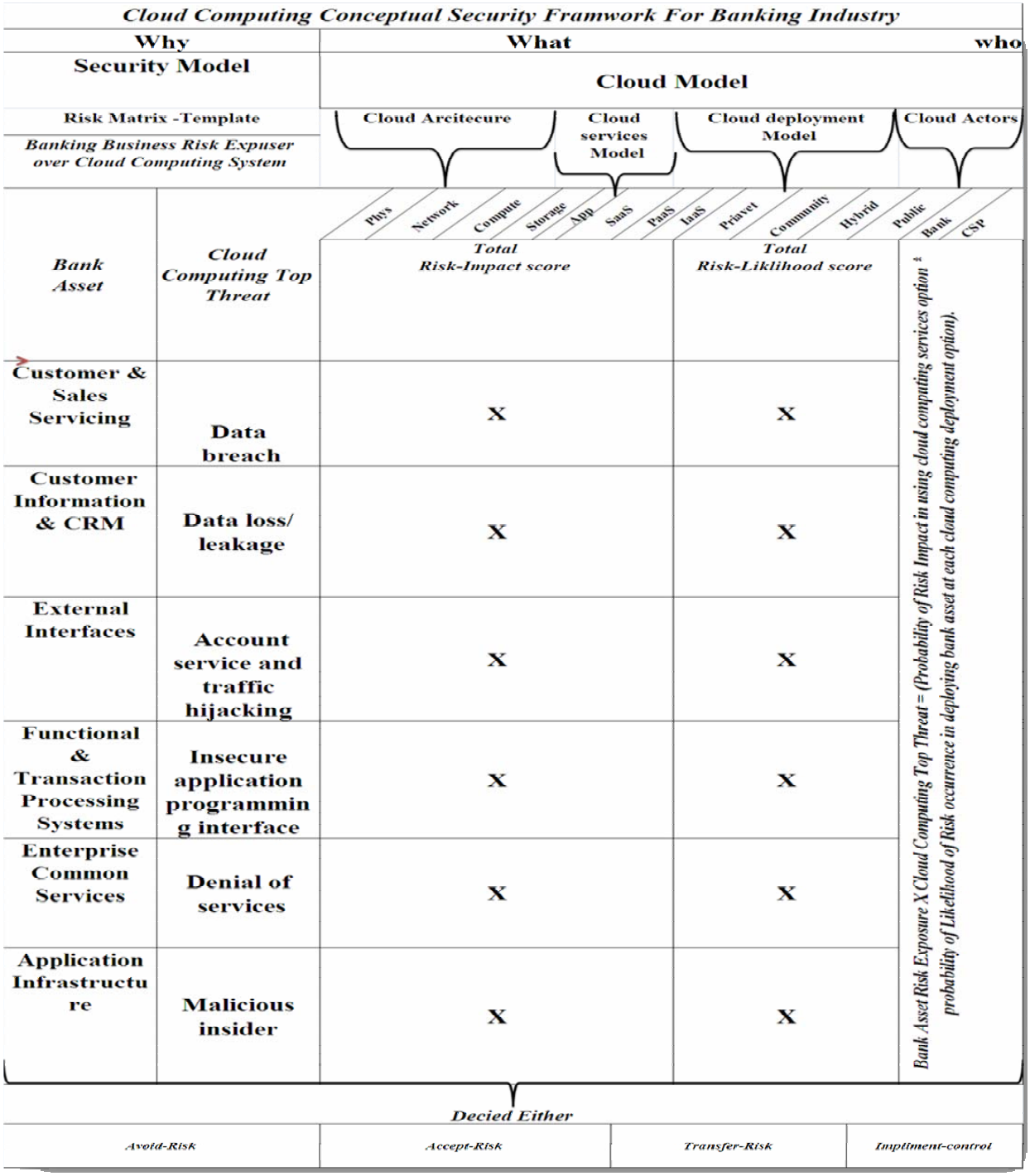

Figure 4: Risk Matrix template- Bank Business Risk Exposure

Compliance Model (How)

In the framework, in order to address legal and regulatory compliance issues, we designed Compliance Matrix Template (see Figure 5). It is developed basing banking industry standards (GLBA, BasleII/II, PCIDS, SOX), cloud computing control matrix and international regulatory best practices compliance requirement (ISO, COBIT, etc.). On the matrix, compliance requirement of those regulators is mapped to each specific control domain.

Cloud Computing Conceptual Security Framwork For Banking Industry					
Compliance Matrix-Template			How Compliance Model Compliance Matrix		
			Bank Industry Standards	Cloud Computing Standards	International Standards
			GLBA PCIDSS SOX BasleII/III	CCM-COBIT ,ISO/IEC 27001-2005, FedRAMP, PCI DSS	ISO HIPPA COBIT
Security Model	Administrativ-Control	Policy Document (Governance, Risk and Compliance)	x	x	x
		Legal	x	x	x
		Personal Security			
		Third party provider	x	x	x
		Business continuity and Resource provision			
	Technical - Control	Network, Host and VM security	x	x	x
		Appliaction security			
		Identity and access management	x	x	x
		Incident Management			
		Data secuity (Transit,storage,rest)	x	x	x
		Operational-managemer			
	Physical Control	Data center- Physical Security	x	x	x
		Data center- Enviromental Security			
		Data Center- Power And Network	x	x	x
		Data center- Human resourse			

Figure 5: Compliance Matrix Template

Based on the compliance matrix template, we designed cloud computing security strategy/major which includes specific tools, products, best practice and guidelines for the banking industry (see Table 1).

Table 1: Security Major Template

Cloud Computing Security Framework For Banking Industry	
Security Major Template	
Policy Document	Governance, Risk and Compliance
Legal	OECP, APEC
Personal Security	
Third Party Provider	
Business Continuity and Resource provision	Plan for managing resources, conduct impact analysis, check power & telecommunication infrastructure, back up-plan, disaster recovery-plan

Network, Host and VM security	*Wireless Network setting*: Perimeter Firewall, strong encryption for authentication & transmission. *Shared Network*: Bank security requirements, compliance with legislative, regulatory and contractual requirements, separation of production and non-production environments, preserve protection and isolation of sensitive data. *Network Control*: *Availability*: Check network architecture, e,g., Load balancing, Cluster architecture, Checkpoint restartor or robustness. *Integrity*: secured hashing algorithm e.g., SHA-512, Digital Certificates. Confidentiality: Strong password policy and access control e.g., 256-bit AES, SSL, SHA and TLS-1.1 *Virtual Machine Gust Hardening*: e.g., using firewall, web application, antivirus, file integrity monitoring & log. *Hypervisor Security*: Physical, operational security for hosting server.
Application security	Storage- Authentication, Digital signature/Hash, SAML, Audit logging, Web-services security get-way, and AAA.
Identity and access, management	RBAC, SSA token, OTP, SAML, XACML, SCLM
Incident Management	SLA, IODEF, RID, CEE
Data secuity (Transit,storage,rest)	DSLC, IDA, Encryption- Clint application, Network (SSL, VPN, SSH), Proxy, DAM, FAM, DLP-Tools, URL Filtering
Operational-Management	Documented operating procedures:-Capacity management, Change management, Exchange of information, System Acceptance.
Data center-Physical Security	Physical Security Perimeter, Resiliency - Equipment Location
Data center-Environmental Security	Smoke Detector & Fire Suppression System
Data Center- Power And Network	AC, Battery, UPS, Fire link detection, Automatic Fire extinguished, Generator
Data center- Human resource	Background Verification & Screening Agent

4. Conclusion and Future Work

The general objective of this research is to develop cloud computing security framework for the banking industry. Accordingly, in order to achieve this objective, detail assessment on cloud computing architecture, reference model, service, threat and attacks, policy, standards and guidelines were done. Similarly, assessment has also been made on bank industry regulatory security and compliance requirements. Based on these assessments to address the research problems we designed cloud computing security framework for the banking industry.

Our framework provides Risk Matrix Template for assessing and determining risk exposure of bank asset applications while moving to cloud deployment option. Integrated control domain component is proposed as a base for setting security major. Finally, for each defined control domain, security major/strategy (tools, products, guidelines and practices) is proposed.

For future work, we recommend automation of main security solutions, Risk Matrix template, Control Domain Template, Compliance matrix template for ease of use and updatability. For future research we also recommend setting maturity model for the proposed security framework.

Finally, banks are recommended to major their business risk exposure before moving their

application/asset/data to cloud deployment models (Public, Hybrid, Community, Private). We also recommend banks to set control major in compliance with regulatory requirements. On the other hand, to move banks to cloud computing more work is required form regulatory standard organization perspectives. This organization should provide and conduct more research and should provide updated security guidelines.

References

[1] David Bradshaw, Giuliana Folco, Gabriella Cattaneo, Marianne Kolding, "Quantitative Estimates of the Demand for Cloud Computing in Europe and The Likely Barriers to Up-take" IDC Analyze the Future, D4 Final report, Ver. 2.0, Brussels, Belgium, SMART 2011/0045, July 13, 2012.

[2] Ollivia La Barrer, "Bank System and Technology," Information week cloud, 2011, retrieved form, http://www.informationweek.com/cloud-computing/software/temenos-microsoft-bring-azure-clouds-to/231002099, Last access on August 15, 2013.

[3] H. Altalhi, Mohamed Sidek, Abdul Ghani, Othman, and Abdelkhaleq Al-Sheshtawil, "Enhancing the Security Framework Secure Cloud with the SWIFT Identity Management Framework", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol. 2, No. 1, February 2012.

[4] IBM, "Security Over View Cloud Computing," Cloud Computing White Paper, United States of America, IBM Corporation, 2009.

[5] Federal Risk and Authorization Management Program, "FedRAMP," CONSOP Briefing, February 9, 2012.

[6] Sunita Rani and Ambrish Gangal, "Security Issues of Banking Adopting the Application of Cloud Computing," International Journal of Information Technology and Knowledge Management, Vol. 5, No. 2, July-December 2012.

[7] Working Group Report on Cloud Computing Option for Small Size Urban Cooperative Banks, Reserve Bank of India, retrieved from http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/ RWGFUF031012.pdf, Last accessed on August 15, 2013.

[8] Working Group, "Information Security, Electronic Banking, Technology Risk Management and Cyber Fraud," Report and recommendation, Reserve bank of India, Mumbai, January 2011.

[9] John Sherwood, Andrew Clark, and David Lynas, "Enterprise Security Architecture" SABSA, White paper, 1995-2009 SABSA Limited.

[10] TOGOF, "The Open Group Architecture Framework," retrieved from, http://www.opengroup.org, Last accessed on August 14, 2013.

[11] SABAS, "The Sherwood Applied Business Security Architecture Framework" Available at http://www.sabsa-institute.org, Last accessed on March 15, 2013.

[12] ISO, "ISO/IEC 27002:2005", retrieved from, http://www.standardsconsultants.com/isoiec-270022005, Last accessed on August 14, 2013.