Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Cloud Computing Conceptual Security Framework for Banking Industry

[1] Meskerem Alemu, [2] Abrehet Omer
[1] HiLCoE School of Computer Science and Technology, Computer Science Department, Addis Ababa, ETHIOPIA
[2] PHD, Addis Ababa University, Department of Computer Science and Technology, Addis Ababa, ETHIOPIA

[1] meskiyir@gmail.com, [2] abrehet@gmailcom

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. Due to lack of professionals and adequate security frameworks in the area, the issue is getting scaled up to become a severe problem. In this research ,through conducting systematic literature review on cloud computing and banking industry security standards, policy and best practices coupled with interview as methods of data collection, we proposed applicable Conceptual Cloud Computing Security Framework for Banking Industry. The Sherwood Applied Business Security Architecture (SABSA) enterprise security model is used as a guide for designing the newly proposed security framework focusing on architects view of five basic security matrix question (What, Who, Why, Where, How). The proposed framework incorporates major component that addresses security, privacy, legal and compliance and regulatory issues.

Keywords: *Cloud Computing, Banking Industry, Security Framework, Security Matrix*

1. INTRODUCTION

In order to satisfy customers need and to deliver better services, 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 been 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.

Researchers [3]-[7] reviled that, adoption of cloud by banks is at infant stage because of security issue as there is no clear standards and frameworks that guide banks in using cloud services. There is no clear framework that shows them where their data resides in the cloud, how their data is secured, and how to select the right service, deployment, and operating models to address security and compliance concerns. Therefore, to move banks into cloud computing environment security, privacy, legal, regulatory and compliance issue in relation to banking services should be address.

This research attempts to answer the research question "what are the suitable security components to propose new Conceptual Security Framework that addressed the security, privacy, legal, compliance and regulatory issues of banking business in adopting Cloud Computing Technology".

The paper is structured as follows: Section 2 describes the prior work done on cloud computing security frameworks and banking industry. Section 3 presents the proposed conceptual Security framework. In Section 4, we describe the component of the proposed framework. We conclude the research in Section 5.

2. RELATED WORK

Cloud Security Reference Model [8] issued by Cloud Security Alliance (CSA) is built based on cloud computing architectural model. This architectural model in turn mapped to a model of compensating security and operational controls; and in turn to compliance standards. The framework focused on providing specific physical and technical control that does not incorporate administrative security risk control related to bank industry compliance requirement.

Similarly, [9] proposed, Novel Open Security Framework for Cloud Computing. In the framework, privacy, trust, Interoperability, CIA, Transparency, Open standards, self-managed security elements is set as an objective to achieve security. However, the proposed framework focused on providing specific security solution which varies through time.

On the other hand, Temenos [10] proposed, Temenos Enterprise Framework Architecture (TEFA). In the framework, Security Management System is incorporated as one component. Since, the framework is not designed basing cloud computing architectural component it does not address security risk related to cloud computing technology. Similarly, IBM [5] was also deliver Security Overview on Cloud computing, in the framework IBM identifies main component in general;

however, the framework is not designed basing cloud computing architecture and banking business security requirements. In addition to this, regulation standards and compliances and the way to adopt cloud computing for banking services is not addressed in the framework.

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" and should consider security as management issue, and should bounded time and detail defense in-depth [12-14]. Based on these facts we can say that previous works on cloud computing security and banking industry security framework does not cover the overall technical, administrative and physical security issues on cloud architecture & banking business operation. Our research addresses this gap through conceptual cloud computing security framework which is developed considering cloud computing security architecture and banking industry security and compliance requirements.

3. PROPOSED FRAMWORK

There is a general agreement among security professionals and expertise that the overall objective of information security is to preserve the availability, integrity, and confidentiality of an organization's information. In order to achieve this objective, we followed Architects View of SABSA model. Architects view layer of the SABSA model is referred to as the Conceptual Security Architecture [15]; it defines principles and fundamental concepts that guide the selection and organization of the logical and physical elements at the lower layers of abstraction. Accordingly, based on banking industry security requirement five basic security matrix questions (what, who, why, where, how) of Architects view are answered in the conceptual cloud computing security framework depicted under figure 1 below.

Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

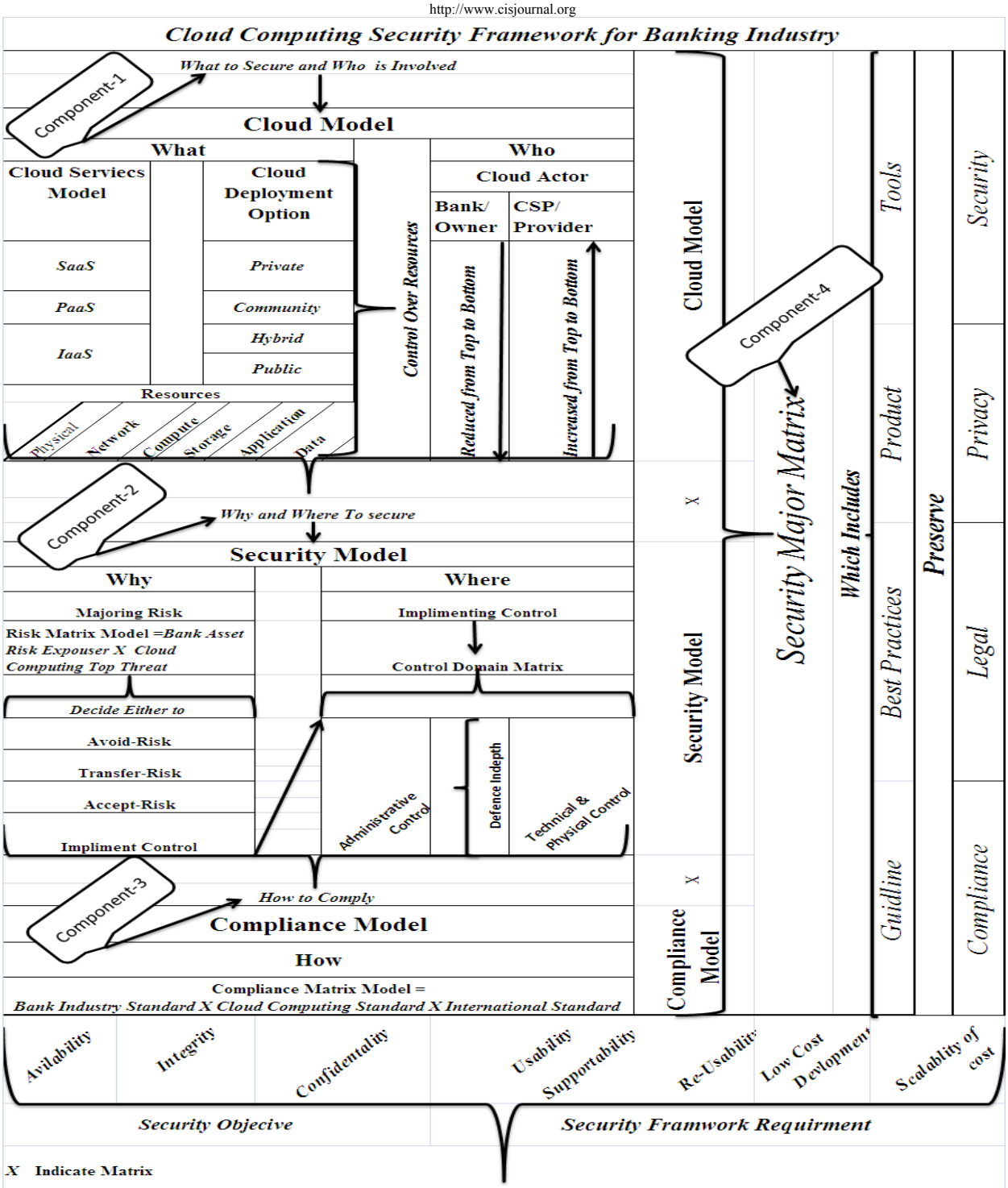

Fig 1: Proposed Cloud Computing Conceptual Security Framework for Banking Industry

Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

4. DISCUSSION OF THE PROPOSED FRAMWORK

The detail discussion of the proposed conceptual security framework components is presented as follows:

4.1 Component 1-Cloud Model (What and Who)

4.1.1 What you want to Protect and who is Involved in the Security Management

Expressed in the SABSA architects view in terms of business attributes, primary business requirement, roles and responsibilities and the type of business trust that exists between the parties including asset owners, custodians, users, and service providers and service customers. Moreover, SABSA states that, enterprise security architectural approach needs a clear understanding of a system. This can be driven from asking questions such as, **What type of system is it** and **Who will use it**?[15] Similarly, according to CSA [8], in developing cloud security framework one has to first consider cloud architectural reference model, then classifying cloud services against cloud architectural model. By doing this it is possible to map its security architecture; as well as business, regulatory, and other compliance requirements against it as a gap-analysis exercise.

Based on this fact, on the Conceptual Framework as presented in figure 1, the first two basic security question **"What to secure and who is involved?**" are answered through **Cloud Model.** This model is set through analyzing Cloud architectural reference model provided by CSA [8] and NIST [16]. In this model, systems that need to be secured and involved parties are identified through analyzing Cloud Computing threat source in terms of responsibility and control over resources. The Identified threat source component includes Cloud Actors, Cloud Services Model and Cloud Deployment Model.

Accordingly, in the conceptual Security framework figure 1 the parties involved in the cloud system are represented with **"Cloud Actor"** which includes **CP** (Cloud Provider) and **Banks (**Business Owner). Similarly, the type of Cloud services and the computing resources at each service is also identified in the Conceptual framework and represented with "**Cloud Services Model**". Moving down to this services model control over resources and responsibility is reduced for banks and increased for CSP. Table 1 below illustrates, the details of computing resources available at each cloud computing services model (SAAS, PAAS, IAAS)1 and control over this resources by **Cloud Actors** (Banks and CP)

Table 1: Control over Resources by Banks and Csp across Cloud Services Model

Cloud Computing Services	Computing Resource Available	Responsible Actor to Control Resources
SAAS	Application	PAAS-Bank, IAAS-Bank, IAAS-CP
PAAS	Libraries , Database, Java, Virtual Machine	IAAS-Bank, PAAS-CP
IAAS	Operating system Devices(Host and Gusts)	IaaS-Bank, IaaS-CP

On the other hand, control lover resources by **Cloud Actors** at each **Cloud Computing Deployment Option** are also indicated in the Conceptual Security framework figure 1. Table 2 below illustrates the detail control over computing infrastructure by **Cloud Actors**. In this Table 2, "Trusted", represents consumer of a banking services those who are in the banks legal, contractual, policy umbrella including employee, contractors and business partner etc. Likewise "Un-trusted" consumers are those that may be authorized to consume some or all services of the bank but are not logical extension of bank resources.

Table 2: Control over Resources by Banks and Csp across Cloud Computing Deployment Options

Cloud Deployment model	Infrastructure Managed By	Infrastructure Owned By	Infrastructure Located	Accessible and controlled
Public	CP	CP	Off Bank premises	Un-trusted
Private/ Community	Bank or CP	Bank or CP	On Bank premises or Off Bank premises	Trusted
Hybrid	Bank and CP	Bank and CP	On Bank premises and off Banks premises	Trusted and un trusted

4.2 Component 2- Security Model (Why and Where)

4.2.1 Why the Protection is Important

Expressed in SABSA architects view, in terms of control and implements objectives. Control and implement objectives are derived directly from an analysis of business operational risks; thus risk assessment should be made against the business attributes profile assets.

In order to deal with "**Why**" security question in cloud computing, banks have to major the risk of deploying each bank asset/application/function/data at each cloud computing deployment and services option.

Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

As shown in the proposed Conceptual Security framework figure 1, we design Security Model and we specified, Risk Matrix Model with a matrix solution as "Risk Matrix Model= Bank Asset Risk Exposure X Cloud Computing Top Threat". Following ISO-27001 [17, 18] we defined Risk Exposure Majoring equation given as follows.

Bank Asset Risk Exposure over Cloud Computing Top Threat can be majored through majoring = (Probability of Risk Impact in using cloud computing services option * probability of Likelihood of Risk occurrence in deploying bank asset at each cloud computing deployment option).

Hence, in order to perform the risk measurement, specific bank asset and top cloud computing threat should be identified and the probability of risk impact and likelihood of risk occurrence should be calculated. In order to deal with these issues, the Risk Matrix Template is illustrated under figure 2 below. In the Template bank asset and top cloud computing threat is specified; so that each bank asset risk impact probability across cloud computing services option should be determined based on the identified top cloud computing threat. Similarly, the probability of risk occurrence in deploying this asset across cloud computing deployment option (Private, Community, Hybrid and Public) should be determined. Then based on the risk exposure result both the CSP and banks has to decide either to Avoid , to Accept , or to Transfer the risk or to Implement Control.

Cloud Computing Management Framwork For Banking Industry

Why	What														Who	
Security Model	Cloud Model															
Risk Matrix -Template	Cloud Arcitecure				Cloud services Model			Cloud Deployment Model							Cloud Actors	
Bank Asset	*Cloud Computing Top Threat*	Phys	Network	Compute	Storage	App	SaaS	PaaS	IaaS	Private	Community	Hybrid	Public	Bank	CSP	*Bank Asset Risk Exposure X Cloud Computing Top Threat = (Probability of Risk Impact in using cloud computing services option * probability of Likelihood of Risk occurrence in deploying bank asset at each cloud computing deployment option).*
		Total Risk-Impact score						*Total Risk-Liklihood score*								
Customer & Sales Servicing	Data Breach	X						X								
Customer Information & CRM	Data loss/ leakage	X						X								
External Interfaces	Account service and traffic hijacking	X						X								
Functional & Transaction Processing Systems	Insecure application programming interface	X						X								
Enterprise Common Services	Denial of services	X						X								
Application Infrastructure	Malicious insider	X						X								

Decied Either

Avoid-Risk	*Accept-Risk*	*Transfer-Risk*	*Impliment-Control*

Fig 2: Risk Matrix Template

After measuring the risk if the parties are decided to implement control, the next question will be where to implement control? According to SABSA, **where you want to achieve the protection** expressed in Architects View in terms of a security domains framework. Important concepts here are security domains (both logical and physical), domain boundaries and security associations. As shown in the proposed Conceptual Security Framework figure 1, **Control Domain Matrix** is set under Security Model. It is a matrix solution for setting control domain over cloud computing resources. Here we provided, **Control Domain Matrix Template** illustrated in the figure 3. In this Template we defines a control matrix solution through defining specific control under the three controls domains (Administrative, Technical and Physical) and mapping this control to each cloud computing architectural resources component which is defined under **Cloud Model**. The mapping is indicated with symbol "X". Control over resources and responsibility of cloud actors (CP and banks) at each cloud deployment option is also clearly defined in the Control Domain Template figure 3. So that in cloud computing environment, this template allows identifying the responsible actor (either banks or CP) to control over resources and allowing where to implement control and the specific control type.

4.3 Component 3- Compliance Model (How)

How you want to achieve the protection: Expressed in SABSA architects view in terms of high-level technical and management security strategies. In order to deal with this issue, we defined Compliance Model under the proposed Conceptual Security Framework figure 1. Compliance Model contains Compliance matrix which is defined to meet legal, compliance and regulatory issues in cloud computing environment. Compliance Matrix Template shown in figure 4 below illustrates how controls can be defined integrating with well-known Cloud computing standards, International standards and Banking industry standards.

4.4 Component 4- Security Major

In order to meet overall security, privacy, legal and compliance requirement in cloud computing,

Security Major Matrix is defined in the proposed conceptual security framework figure 1. It is a matrix solution set through integrating the three models (i.e. Cloud Model, Security Model and Compliance Model); so that, in cloud computing environment specific major should be set considering the cloud architectural component and control should meet bank industry standards, cloud computing standards and other international standards. Table 3 below shows the Security Major Template which is defined for setting specific security major which includes specific tools, products, best practice and guidelines.

Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

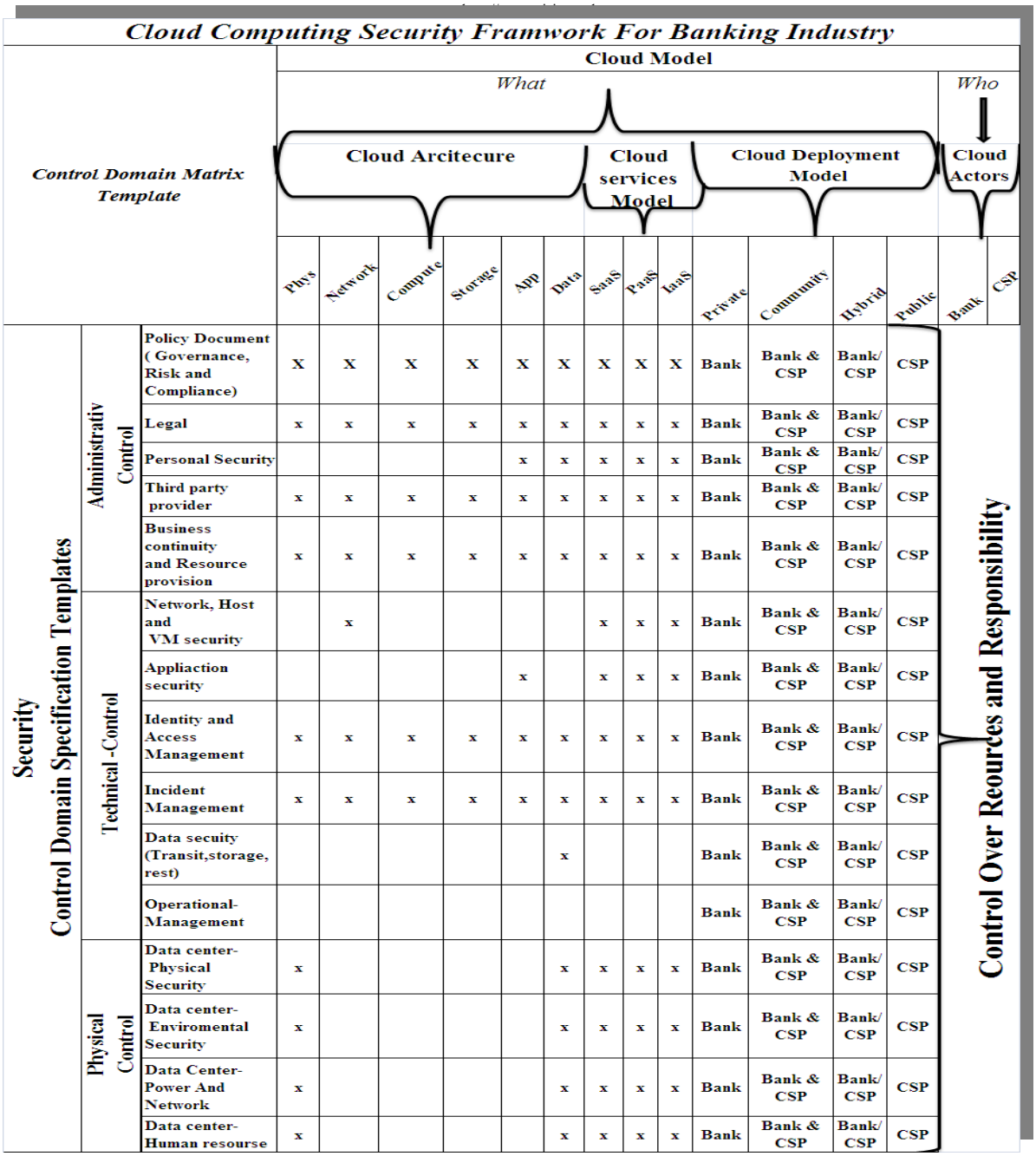

Fig 3: Control Domain Matrix Template

Vol. 5, No. 12 December 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

Cloud Computing 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 Management			
	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			

Fig 4: Compliance Matrix Template

Table 3: Security Major Template

Cloud Computing Security Framwork For Banking Industry	
Security Major Template	
Policy Document	Governance, Risk and Compliance
Legal	OECP, APEC
Personal Security	
Third Party Proviedr	
Business Continuity andResource provision	Plan for Managing resources, Conduct Impact analysisCheck Power&Telecommunication infrastructure, Back up-Plan, Disastor recovery-Plan
Network, Host and VM security	**Wireless Network setting**:-Perimeter Firewall, Strong encryption for Autentication & transmition. **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:- Avilablility**:- Check network Arcitecture eg. Load balancing,Clustor arcitecture, Checkpoint restartor or robutness**. Integrity**:-secured Hashing algorizm eg.SHA-512, Digital Certeficats**. Confidentiality**:-Strong Passward Policy and access control eg.256-bit AES,SSL,SHA and TLS-1.1**Virtual Machine Gust Hardening**:- eg. using Firewall, webapplication,antivirus, file integrity monitoring &log.**Hypervisor Security**:-Physical, operational security for hosting server.
Appliaction security	**Storage- Authentication, Digital signature/Hash, SAML, Audit logging, Web-services security get-way, and AAA.**
Identity and access, mangment	**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-Enviromental Security	Smoke Detector & Fire Suppression System
Data Center- Power And Network	AC, Battery, UPS, Fire link detection, Automatic Fire extinguished, Generator
Data center- Human resourse	Background Verification & Screening Agent

5. CONCLUSION AND FUTURE WORK

The general objective of this research is to develop cloud computing Conceptual Security Framework for 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 assessed. Similarly, assessment has also been made on bank industry regulatory security and compliance requirements. Based on these assessments we designed Conceptual Cloud Computing Security Frameworks for Banking Industry see Fig.1. Our proposed framework addresses security, privacy, legal, compliance and regulatory risk though identifying and representing systems that need to be secured in cloud system with Cloud Model, and in order to preserve security and privacy, major security component is identified and represented with Security Model. To facilitate meeting legal and compliance issue Compliance Model is set. More so, in the framework Risk Matrix is set for assessing and determining risk exposure of bank asset applications while moving to cloud deployment option. Moreover, integrated control domain and compliance model component is also proposed as a base for setting security major. Finally, for each defined control domain, security major/ strategy (tools, products, Guidelines and Practices) is proposed shown in Table 3. 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. 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 and et.al "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] 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.

[4] Takabi, H etal, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments," in the preceding of IEEE 34th Annual Conference on Computer Software and Application, July 2010.

[5] Ec. Mihai-Florin Talpo, "Strategic Role and Importance of the Remote Access Financial Solutions for Banks' Activities," Abstract of Doctoral Thesis, Faculty of Machine Building, Technical University of ClujNapoca, 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, "Information Security, Electronic Banking, Technology Risk Management and Cyber Fraud," Report and recommendation, Reserve bank of India, Mumba, January 2011.

[8] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, Vol. 3.0, published in 2011, retrieved from http://www.cloudsecurityalliiance.org /guidance/csaguid.v3.0.pdf, Last Accessed on August 15, 2013.

[9] DevkiGaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh, "Novel Open Security Framework for Cloud Computing" International Journal of Cloud Computing and Services Science (IJ-CLOSER), Vol.,1, No.2, June 2012,

[10] Temenos, "A New Way for Banking System Architecture: Temenos Enterprise Framework Architecture," Temenos White Paper,2012 Temenos Headquarter SA

[11] IBM, "Security over view Cloud Computing," Cloud Computing White Paper, United States of America, IBM Corporation 2009

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

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

[14] Marshall B.Romneyand Paul John setinbart, "Accounting Information System" Ed 11, Prentice .Hall 2009.

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

[16] Fangliu, Jin tang, Jian Mao, Robert Bohn," Cloud Computing Reference Architecture" National Institute of standard and Technology special publication 500-292, September 2011.

[17] ISO Risk assessment and treatment, retrieved from http://privacy.med.miami.edu/glossary/ xd_iso_risk_assess_treat.htm, Last accessed on August 14, 2013.

[18] Public risk management association "Enterprise Risk Management (ERM) and the requirements of ISO 31000"AIRMIC, Alarm, and IRM, 2010

AUTHOR PROFILE

Meskerem Alemu received her MSc. degree in Computer Science from HiLCoE School of Computer Science and Technology, in 2014. Currently, she is working at Bank specializing on IT security.