Governance Life Cycle framework for Managing Security in Public Cloud: From User Perspective

Rizwan Ahmad
Information Systems and Operational Management
University of Auckland
Auckland, New Zealand
r.ahmad@auckland.ac.nz

***Abstract*—Public Cloud Computing (PCC) delivers technology "As a Service". It is widely accepted by consumers, enterprises and, even governments because it reduces financial budget for acquiring Information technology (IT) infrastructure. The major deterrence against its adoption is security and governance risks. These risks are associated with three facets; geographical location of cloud provider, change of governance level within cloud service layers and inadequacy of existing international security standards to maintain security. In this paper, these three domains are researched to formulate governance life cycle framework for managing user data security in PCC.**

Keywords-Cloud Computing; Governance; Security; Management

I. INTRODUCTION

The cloud computing is a natural bricolage[1], an amalgamation of existing technologies to benefit users[1]. It is commonly known "as a Service" model [2, 3], comprised of technological nodes that are coordinated systematically to perform services for user in the form of software, platform and infrastructure provided by Cloud Provider (CP). It follows "pay for what you use" model. The commonly accepted definition is from National Institute of Standards and Technology (NIST) that defines it as " Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is comprised of five key characteristics, three delivery models, and four deployment models".

PCC inherits its name from one of the four deployment models defined by NIST, private, public, community and hybrid. PCC is available for public at large and ubiquitously located anywhere in geographical domain. Amazon (EC2), Sale Force (Force.com), Google (Google apps); Microsoft (windows Azure) has their supporting data centers at different places in the world are examples of PCC. It is delivered by three service layers Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [2-6]. The user does not buy IT infrastructure, software and or pay for software licenses. CP provide rapid allocation of resources and instant scalability[5, 7]. These characteristics save money on IT infrastructure procurement, software with peripheral licenses, its maintenance and up gradation[8]. It is an ideal model for users getting IT support from CP to process their data. ISACA survey validates that enterprises are embracing cloud computing to cut IT cost and expenditure [9]. However, these benefits are outweighed by governance and security risks [10-14].

The main focus of paper is protection of user data and posits pre and post governance framework for adoption of PCC. The framework is developed from relevant clauses of international standards[2] and legal principles, the two important drivers that have shaped overall structure of computing. The legal precedents are considered to strengthened technical aspects and security considerations for three reasons:-

- To evaluate and validate governance framework from legal perspective
- To strengthen security standard clauses to protect user data
- To provide a holistic management framework that can be generalized and applied in different jurisdictions

The following sections will describe lack of governance and associated security risks by considering three domains; cloud service layers, security standards and law. Section 2 will define governance considering different views and explain the risks associated with PCC. Control variation within the cloud layers that affect governance will also be described. The section 3 will describe initial development and analysis of governance framework followed by elaborated section 4 dealing with framework and its discussion, and ending as conclusion in section 5.

II. ISSUE OF GOVERNANCE RISKS

Governance has its origins from Greek verb κυβερνάω [*kubernáo*] which means to govern, steer, devise guide

[1] User or users is defined in this article as consumers, small and medium size enterprise or Enterprises using the cloud services

[2] The standards when referred in this paper will include international standards ISO27001/2, COBIT, PCI-DSS, NIST 800-53 rev3, HIPAA

control[15]. It was first used by Plato to design a system of rules. The other definitions, governance is system of rules, exercise of power and control[16]. In IT, governance is associated with "responsibility of the Board of Directors and Executive Management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives". Weill et al defined IT governance is about specifying the decision rights and accountability standard to encourage desirable behavior in using IT[17]. It is widely accepted that IT governance is responsible for two main functions; it delivers value to the business and mitigation of IT risks [18, 19]. IBM defines it as "a process that establishes chains of responsibility, authority, and communication, to empower people, as well as measurement and control mechanisms to carry out their roles and responsibility". All these definitions correlate some form of control to obtain desired behavior by implementing set of rules to exert responsibility, incorporating through strategic decisions and creating deterrence through accountability. In computer systems, the desired behavior is achieved by applying security architectures in operating systems, integrating software security best practices while developing software and integration of security governance within enterprise to control processes to perform desired tasks. In a distributed environment, like cloud computing, governance is application of technical security controls and developing set of rules or policies that reflects the intention of users and CP, to protect data and managing shared responsibilities.

These definitions are an integrated features of existing security standards ISO27001/2, CoBIT, NIST 800-53 rev3 and PCI-DSS. These standards offer governance and security integration within an organization that owns the assets people, process, software and hardware. The responsibility within these standards is associated with the owner[3], responsible for security of asset approved by management. The declaration of an owner within architecture of cloud computing may be misleading especially on PaaS and IaaS layers. The level of control changes within these layers, it shifts from CP to user while using SaaS, PaaS and IaaS. Though the user owns the information assets but these are processed on transnational IT infrastructure of CP. For critical business application, transnational nature of PCC, pose a security threat and loss of control. The standards are silent on this issue and do not adequately exemplify clauses of control that illustrates governance. However, the portion of these standards relevant to PCC is third party clauses, which legally possess threat to data leakage recognized by precedents. Third party doctrine, as interpreted by law courts in USA, makes PCC as an undesirable model for critical applications. The United States Supreme Court has ruled out in Miller[20] case that "*The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed*". Therefore, if CP provides information about user to public authorities or anyone else, it will deprive user's right to security of data. It makes cloud computing much more complex. Its complexity increases especially if CP resides in a country ruled by laws that does not recognize privacy rights.

[3]Owner is a person or entity that has been given formal responsibility, by management, for the security of an asset or asset category. It does not mean that the asset belongs to the owner in a legal sense

A. Variation and Assessment of Governance in Cloud layers

The discussion of governance issues in cloud environment is divided into three logical layers of cloud, SaaS, PaaS and IaaS.

1) Software as a Service (SaaS)

It is supported by the underlined layers of PaaS and IaaS. The user application is developed and maintained by CP. The user accesses it through the web browser [21-23]. The control and security is high because overall responsibility belongs to CP except for some functions described in Table 1. SaaS is cloud computing and can be compared with out sourcing. The standards accommodate SaaS under third party clauses.

Table I. Governance Level on the SaaS layer[13].

Governance Level SaaS Layer	
User Responsibility	**Cloud Provider Responsibility**
Identity Management	Ownership of physical structure
Access Control Policy	Physical security
Authentication	Management of software security
	Management of network security
	OS patch management
	Incident response and resiliency
	Monitoring and Maintenance
	Compliance with standards and legal regulation

2) Platform as a Service (PaaS)

The layer gives developers to customize, develop and deploy cloud applications. It gives more control and authority to user. CP provides APIs and control boundaries for development environment, essential to enhance the application productivity and performance. Control level for CP is decreased and more control is associated with user. The user follows the software development lifecycle (SDLC) to develop, test and maintain his application. User can develop customized application and imply security for his critical applications. The responsibility of due care and due diligence to maintain security of application is exclusively dependent on user. It raises risk of running malicious code, causing disruption to servers and may penetrate the layers that are securely separated by hypervisors[24]. Standards handle malicious code by control 10.4.1 in ISO 27002. It states to have formal policy and deploy software to prohibit such an incident occurring from malicious code. However, question remains open on this issue, who is responsible and liable for breach of due diligence of software. Table 2 illustrates the variation of governance.

Table II. Governance Variation at PaaS[13]

Governance Level PaaS Layer	
User	**Cloud Provider**
Maintenance of Application	Ownership of physical structure
Identity Management	Physical security
Compliance to privacy acts and data protection laws	Management of network security
Authentication	OS patch management
Development of software	Incident response and resiliency
Testing of Software	Monitoring and Maintenance
Maintenance of software and software security	Compliance with standards and legal regulation
Compliance with law related to malicious software	

3) Infrastructure as a Service (IaaS)

It is the lowest layer and user level of control is increased. The user uses his choice of operating system, deploys his applications and store information assets. The user is responsible for operating system, development and storage platform configuration. His responsibility increases to deploy logical security to protect the information and apply his security policies.

Table III. Governance level at IaaS layer[13]

Governance Level IaaS Layer	
User	**Cloud Provider**
Maintenance of Application security policy	Ownership of physical structure
Identity Management	Physical security
Compliance to privacy acts and data protection laws	Management of network security
Authentication	Incident response and resiliency
Testing of Software	Monitoring and Maintenance
Maintenance of software and security	Compliance with standards and legal regulation
Compliance with law related to malicious software	
Configuration of logical security platform	
Configuration and maintenance of guest operating system	

All previous tables show transition of logical control from CP to user which divides responsibility, control, authority and security. SaaS level shows minimum control by user. It increases gradually to gain maximum aperture at IaaS level. The control of physical hardware is out of user domain. These shifts create gap between delegation of responsibility measured by due care and diligence controls. The responsibility is partially shared by both user and CP, however in case of breach, the question of liability as to who is responsible will remain unresolved. Similarly, physical ownership of software and hardware remains with CP. In this state, the user data is exposed to surveillance, insider attack, leakage and infringement of intellectual property right. The transnational nature of PCC adds catalyst to such risk exponentially.

B. Existing International Standards for Governance

The standards are meant to implement security and governance best practices within the organization aligned with the company strategy [18, 19]. These standards enforce security controls to achieve appropriate security level, approved mandatorily by its governance board. The intention of controls in these standards is to maintain governance, control and transparent accountability.

These standards agree to have security policy, asset management, ownership, security awareness, application of security controls to maintain the security at all levels. One of the key aspects is securing the information asset important for user. In PCC information assets are ostensibly owned by user and choreographed on servers of CP. In this case, user is dependent on CP for due diligence. The standards were made for organization so that controls can be equitably applied to reduce the security risk below appropriate residual risk. PCC environment is based on shared responsibility of user and CP manifested by its service layers. Despite CSA has defined unified controls for PCC to address this issue, controls are still to be developed for each service layer. CSA matrix[25] was evaluated statistically, which include standards ISO27001, COBIT, NIST 800-30, HIPAA, PCI-DSS and following was findings:-

- User is inadequately protected
- CP is in position to provide security
- 83% of security controls are applied by CP
- 17% of the security control support user
- The absence of governance controls for user
- Absence of governance board to sanction and accept responsibility

C. Legal Issues and Governance

The scandals like Enron influenced governments to legislate statutes that can safeguard the rights of the stakeholders. These statutes are meant to execute legal auditing to maintain the integrity of the transactions. It forms a major driver to force organizations to comply with existing state laws for safe financial reporting. For example Sarbanes-Oxley act 2002 (SOX) [18] has clauses that requires financial officer and chief executive to attest the accuracy of the financial reports[18], companies must evaluate its internal controls through rigorous auditing and implement the segregation of duties. User cannot implement the legal artifacts of SOX because the data is outsourced to CP, it will be more difficult to follow regulatory compliance while CP resides in the jurisdiction that does not comply with user's country law. Similarly Gramm-Leach-Bliley Financial Modernization Act (GLBA) directs the financial institutions to ensure protection and security of customer information, against unauthorized accesses and

privacy. Similar provisions can be found in European Union(EU) directives, 4th Amendment of United States constitution, Canada[26], UK[27, 28], EU[29], Australia(The Privacy Act 1988) and New Zealand (Privacy Act 1993, Health Information Privacy Code 1994, Telecommunications Information Privacy Code 2003, Credit Reporting Privacy Code 2004). The possible risks could be summarized as:-

- The auditing and compliance to law can be merely impossible to observe by both CP and user. The reason can be existing law, distance and conflict of laws. One example is EU Directive 95/46/EC that prohibits data transfer outside European Union.
- There have been legal precedents which affiliates "public" with third party[30] risks and defendant is denied legal remedy [31]
- The local laws where CP resides may not protect the rights of user and vice versa
- SOX, CLERP etc laws ensures that the financial reporting must be signed by the user enterprise board members to ensure internal controls health
- The gathering of evidence by the forensic team may arise legal implications that cannot be addressed immediately especially under PATRIOT act and UK Regulation for of Investigatory Powers Act 2000 (RIPA). These acts require internal authorization to access the data for evidence, this robs user from his right of protection
- CP might enforce contractual obligation to disable migration of user to any other CP
- GLBA requires the protection of identifiable financial personal information by service organization

III. Framework for Cloud Management and Governance

The literature review of cloud layers, existing standards and legal implications purport that PCC requires multi-faceted governance and management framework to secure user, cloud provider and business running on machines. The multi approach includes the clauses of statutory law, clauses of standards and IT controls to preserve cloud security and governance. The success of the model depends on the statutory principles that are integrated within the applied security controls and contractual agreements. The international standards need improvement to maintain the best practices within the clouds. Similarly, law is still to be shaped to address technical as well as jurisdictional issues of PCC.

A. Research Method Used

It is almost vital to protect user data to establish the successful concept of cloud computing. The critical applications require security level that is well above baseline security controls, and it needs more cautious effort when applying to PCC. From the previous literature we can assess that PCC does not have only technical issues but also spawned with legal flaws. The application of security controls to protect the user data will not be completed until it is backed and strengthened by law. Therefore the research method used to develop the governance life cycle involves security standards and legal interpretations. The common set of rules and controls were classified from standards that can sustain governance. Thus controls in these standards verify compliance[20] with law, however it was necessary to use law holistically to positively protect user data and add accountability.

B. Alignment of IT, Standards and Law

The major obstacle in PCC is the conflicts of law of various jurisdictions. In the model, statutory laws were considered rooting from common jurisprudence. Therefore choice of legal study was UK, USA, Australia and New Zealand. Most of the statutory laws enacted in these countries are part and parcel of common law.

The three domains standards, PCC service layers and Law need an alignment with each other to mitigate the security risks. The intersection surface in Figure 1 presents probable variables that can mitigate risks and secure both parties. The model covers the relationship of user and CP from three angles, auditing, liability and operational security. The classification within these intersection areas are based on common and accepted rules of statutory laws of different countries, artifacts of cloud service layers and security standards. The triangulation of liability, audit and operational security is used to produce set of rules that are essential for governance of relationship between user and CP. In the figure 1, the horizontal and vertical assurance is alignment between IT security standards and cloud services models. The main objective is to glue standards, technical controls and law to deliver governance and security.

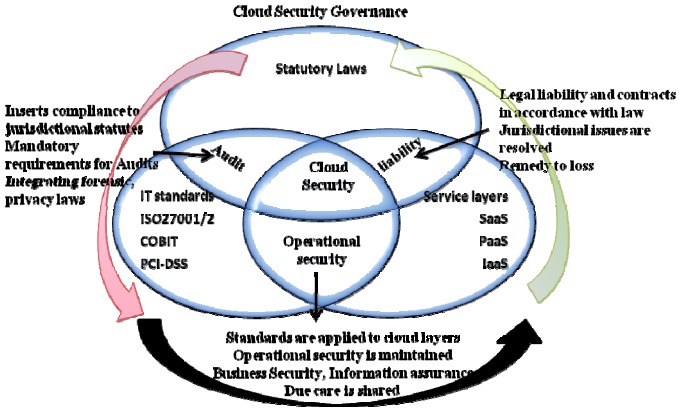

Figure 1. Cloud Security Governance Model

The final framework was developed from figure 2. The statutory study was undertaken considering privacy acts, constitutional rights and financial law in various countries, supported by case law precedents. The outcome was the classification of law that can suit both user and CP, understandable by local courts and can be translated to IT controls to provide security and assurance.

Unified approach was used to classify standards into different domains. If one of the standards is not able to handle that domain, the control of other standard is used and unified

into one framework. The controls were divided into operation, technical controls, management controls and legal controls.
The last domain is the cloud layers itself. The abstraction was applied on each layer so that the unified controls of standards and legal controls can be applied to fortify the cloud governance. The legal controls can be hardcoded in the standard to produce compliance, confidentiality, integrity and preserve the privacy on different layers. Similarly with the technical controls, SLAs and contracts are also outcome from the layers. The user and provider both can write the legal terms to protect their rights under common legal principles available in local law. Figure 2 also illustrates research road map initially examined to produce a governance lifecycle.

C. *Analysis to Determine Governance Life Cycle*

Figure 2 is the research map which was followed extensively. The law of four countries was studied in correlation with standards. It helped to devise governance lifecycle as best practices to protect user critical data. The analysis is shown in table 4.

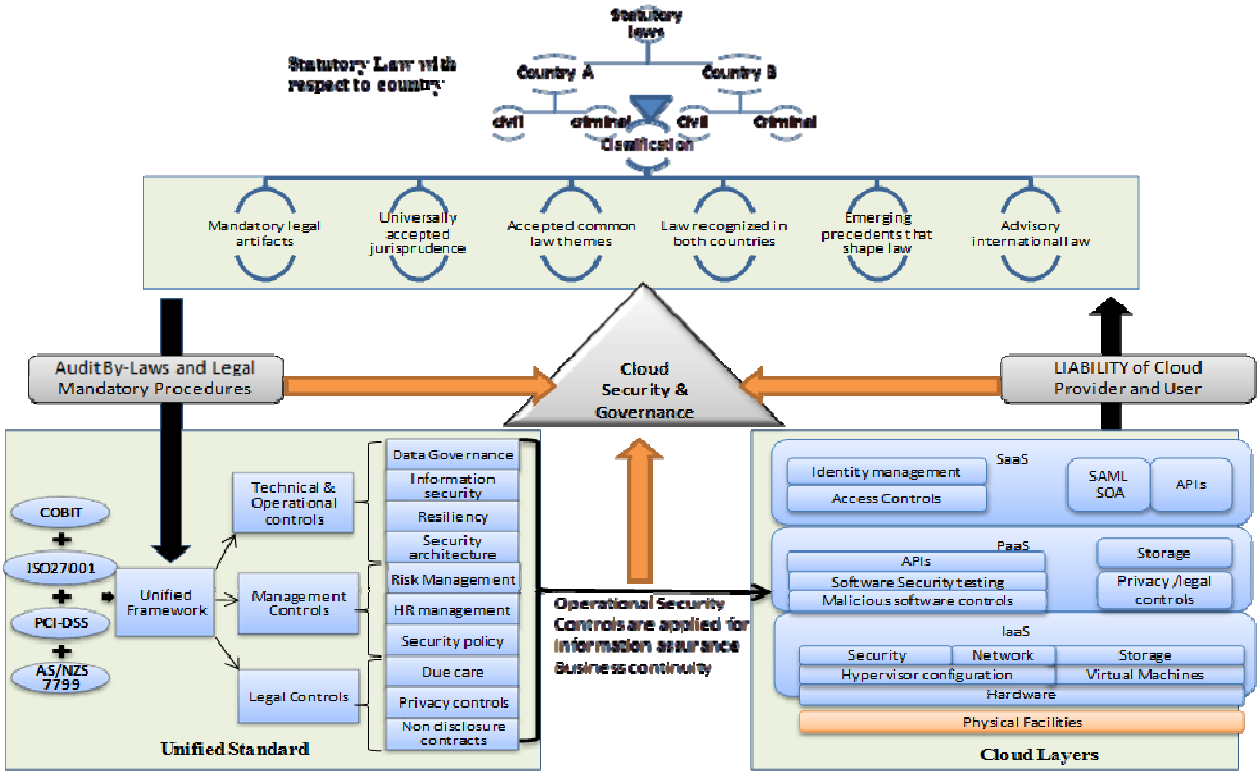

Figure 2. Expansion of Alignment of IT, standards and law for Governance and cloud security

Table IV. Analysis of international standards .considering different domains

Analysis	Explanation	ISO27001/2	COBIT 4
Information security management program (ISMP)	The standards emphasize existence of ISMP that is duly approved, documented and implemented. Legal requirements are mentioned in GLBA ACT 15 USC 6801(B), FTC SECTION 314.3, HIPAA 164.308(a)(1)(i), HIPAA 164.308(a)(1)(ii)(B), HIPAA 164.316(b)(1)(i), HIPAA 164.308(a)(3)(i), HIPAA 164.306(a) *In cloud, the security policy is initiated and implemented by CP. The information about the security measures are not known to user. It is appropriate at SaaS level, CP having direct involvement with the user. However, the development of such program needs approval of user at PaaS and IaaS layers, as user is customizing the platforms for his own use.*	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.1.7, 6.1.8	DS 5.2, 5.5
Security Policy	Approval of security policy by management and aligned with enterprise strategy. Periodical review of policy along with dissemination for organizational awareness Managers are responsible for awareness and maintenance of security policy Legal requirements can be depicted from GLBA 15 USC 6801 (B) (2), HIPAA 164.316(a), HIPAA164.316(b)(1)(i), HIPAA 164.316(b)(2)(ii), HIPAA 164.308(a)(2) EU DIR 95/46 Article 25	5.1.1, 8.2.1, 15.2.1	DS 5.2, DS 5.3, DS 5.4, DS 5.5

	The security policy can be initiated on the infrastructure which is physically in possession of CP. Therefore security policy is enforced at SaaS level by CP. At SaaS CP owns physical and logical infrastructure. At PaaS and IaaS, the implementation of security is divided between User and CP. The standards are silent on this issue. Similarly periodical review of policy, policy awareness is under CP, which is not known to user		
Risk Management	Risk management should be initiated mitigate risk to acceptable level. It also includes risk management program. Legal requirements are mentioned in FISMA 3541(2), HIPAA 164.308(a)(8), 164.308(a)(1)(ii)(B) *However, the standards do not state the authority that will perform risk assessment in cloud layers or on information asset of user. Risk assessment related to people, hardware, software and information asset can be performed by CP at SaaS level. At PaaS and IaaS level, the responsibility for information asset is user's responsibility. There is no designated owner of information assets. The standards give two different views, one is owner defined by ISO27001/2, which is already explained in the paper, and the other is Process ownership defined by COBIT. Process Ownership belongs to the person who performs the services with respect to ownership he possess. For example applying data protection controls over the asset user owns.*	4.1, 4.2	ME 4.5, P09
Asset Management (Data)	The information asset will be assigned an owner; responsibility will be assigned accordingly and documented. The standard define owner as "Owner is a person or entity that has been given formal responsibility for the security of an asset or asset category. It does not mean that the asset belongs to the owner in a legal sense"*In cloud, information asset is critical for use especially at PaaS and IaaS level. These are processed over CP infrastructure which makes both of these entities responsible. However in cloud need pre and post risk assessment of its information asset so that proactively security controls can be approved by user and applied for mitigation of risks*	7.1,7.1.1,7.1.2 ,7.1.3	DS 5.1
Asset Management (Data Protection)	Security procedures should be established to handle data security, retention, disposal and intellectual property. *In cloud, many CP perform data disposal procedures excluding user from SaaS, PaaS and IaaS layers. User does not have any control over his data how it is procedurally maintained, disposed and legally protected with the CP environment. There are some technical functions that are directly protected by the statutes; these are copyright and intellectual property rights. From the user perspective, at PaaS layer, user has the development environment and continuously creating new software essential for their company. It automatically envisages copyright and intellectual property rights that need to be protected by the technical controls of CP or law.*	7.2.2, 9.2.6, 10.1.4, 10.5.1, 10.7.2, 12.4.2, 12.5.1, 12.5.4	PO 2.1, 2.2, 2.3, 2.4
Compliance & Audit	Independent audits and compliance to be performed with relevant standards and law. The legal requirement is HIPAA164.312 (b), SOX Sec 302 (a) (4) (C) and (D). *In cloud, data extraction of data for auditing may lay in different legal jurisdiction. Compliance to SOX, HIPPA, EU directives, UK laws etc requires more coordination and acceptance by both entities. The financial stability and health of internal controls of the cloud provider is another important fact which needs to be evaluated before moving to the cloud. The audit report SAS-70 with SAS-88 is important to be analyzed by user. The standards are silent on these issues*	6.1.8	DS 5.5 ME 2.5, 2.6, 3.1,3.2
Legal Agreements	The direct or third party agreements which directly or indirectly impact on information assets, the contracts must cover all security requirements, liability and dispute resolution. Define and implement a process to ensure timely identification of local and international legal, contractual, policy and regulatory requirements related to information, information service delivery, including third-party services and the IT organization, processes and infrastructure. Further requires positive assurance to compliance. Legal requirements can be depicted from Hague Convention Choice of courts agreementBerne Convention (1971), Right of reasonable expectancy of privacy, Data Protection against third party, European Union, 93/13/EEC (UNFAIR TERMS) *In cloud, CP exercise more authority in terms of contracts and agreement. The terms are defined in a way to advantage CP. CP is flexible enough to make any changes to the contract, which may affect user data. There have been jurisdiction clauses that in event of any dispute, choice of law or place of litigation. For example Google documents* c*ounty of Santa Clara, California as place for litigation[32].*	6.2.3, 10.8.2	ME 3.1, 3.2, 3.3, 3.4
Monitoring	Audit logs recording regarding user whether authorized and unauthorized, may be retained, complying with applicable policies and regulations. Audit logs shall be reviewed periodically. Access to the logging information is in line with business requirements in terms of access rights and retention requirement *In Cloud, CP monitors the data and does not disclose the information to the user nor gives any interface that can access the log reports. While monitoring, the formulation of such policy CP does not include user. The security incidents are also not disclosed. There is a need for bilateral arrangement for agreed monitoring strategy*	10.10.1, 10.10.2, 10.10.3, 10.10.4, 10.10.5, 15.2.2	DS5.5
IT Governance Framework	Work with the board to define and establish an IT governance framework including leadership, processes, roles and responsibilities, information requirements, and organizational structures to ensure that the enterprise's IT-enabled investment programs are aligned with enterprise's strategies and objectives. ISO 27001/2 point to management commitment to information security. Legal requirements mentioned in SOX (302), HIPAA 164.316(b)(2)(ii),164.316(b)(2)(iii), CLERP9, FISMA 3543, European Directive *In cloud, there is no established governance framework which is aligned with the enterprise strategy. CPs provides the interface to the user to access and use the cloud layers to process the data. There is a need for joint board to establish governance so that it should provide value to*	6.1.1, 6.1.2,6.1.3	ME 4.1, 4.2

	business, enforce security, accountability, business process reengineering and resolve issues. In some cases, it is legal requirement to have board so that they should be held responsible especially for critical assets. The corporate law also requires formation of board to devise responsibilities and implement company polices. In security implementation, it is common principle which is supported by standards to use top down approach. This is only possible if there is some responsible management board.		

IV. GOVERNANCE FRAMEWORK

The above analysis shows that existing standards are more centralized to disperse control to manage governance and security in tightly control mechanism. The control over the cloud layers, its jurisdictional nature and security implementation needs co-ordination between CP and user to handle, security of information asset, compliance and accept jurisprudence of distinct jurisdiction. The existence standards can be used together to form security baseline controls, however, the governance model for PCC has yet to be developed for implementation of enterprise governed strategy to mitigate risks for critical application. Figure 3 gives the governance framework.

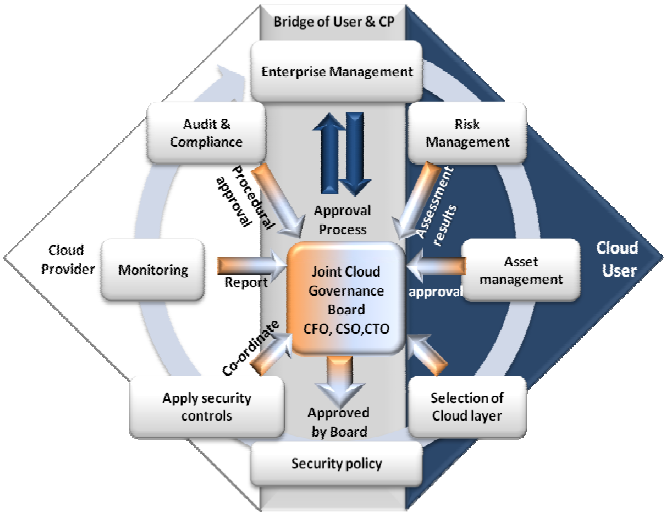

Figure 3. Governance Framework

The framework is divided between two parts; one is followed by user (right side pre-implementation) and other by CP (left side post-implementation). The gap is covered by incorporation of Joint Governance Board (JGB) which is a bridge and central authority for approving various functions during governance lifecycle which includes risk management, asset management, security policy, monitoring, audit and compliance. The cycle from right to left goes from user to cloud provider accepting the responsibilities necessary to accomplish security and governance. In the previous sections, the shift of control was illustrated through the tables; the framework has incorporated these functions from right to left to manage balance and shared responsibility in controlled fashion. The artifacts are explained as follows:-

A. Joint Cloud Governance Board (JGB)

The major obstacle to security assurance in cloud computing is gap between CP and user. The initial step in the governance framework is incorporation of JGB, allowing members from CP and user enterprise. The joint board will be responsible for analysis, approval and implementation of risk management, asset management, and choice of cloud layer, security policy, monitoring, audit and compliance throughout governance life cycle. The existing management literature, legal statutes and standards purports JGB as a governance mechanism to manage, control and mitigate risks. In the management literature, while specifically dealing with other companies, the behavior of organizations is guided by formal contracts for desired expected behavior, legally protected by law[33] and relational governance that steer relationship to accomplish a desired objective on basis of trust. The establishment of JGB extends this idea of incorporating formal contract and relational governance to implement good governance, desired security controls and rules to mitigate the risks. The IT governance literature incorporates responsibility associated with board. Further, the requirement for a governance board is also mentioned in statutes, SOX, corporate laws for responsibility and accountability.

The joint board is a bridge that develops formal control and relational governance between CP and user to demonstrate smooth working co-ordination aligned with user strategy. The joint board is responsible for:-

- Ownership of critical information assets
- Implementation of clear security policy
- Responsible for any acts and commitment that are practiced within the cloud environment
- It also insures that user have the knowledge how users data is protected while using the services of CP
- Responsible for user awareness of security policies
- It is responsible for alignment with local laws, standards and relationship of entities
- Responsible for arbitration and dispute resolution
- General body to formulate contractual terms and service agreements

B. Risk Management

The user is responsible for risk management. It includes the pre and post risk evaluation before and after adoption of the cloud. It follows following two steps, Risk assessment of CP and risk assessment of user information asset.

1) Risk Analysis of Cloud Provider

The first step is to evaluate CP potential to provide business continuity and information assurance in cloud layers. The user evaluates CP qualitatively and checks his credential against the prevailing security standards. This can be ascertained through CP's internationally acclaimed security certification like ISO27001/2 along with the reputation and trust earned. The risk of financial stability is assessed through International Standard on Assurance Engagements (ISAE) 3402 or Statement on Standards for Attestation Engagements (SSAE) 16 Type II. It also verifies the inner health of technological controls running within the physical infrastructure and it is done by the independent auditor. It is also in compliance with SOX and report gives assurance about controls and adequate level of security of CP. Further for financial services, CP privacy controls can be assessed under ISO 22307. These reports will be evaluated by JGB to determine the control effectiveness and cloud feasibility for adoption

2) Risk Assessment of Assets

In cloud computing, the main asset of user is information asset. The remaining asset people, hardware is under CP obligation. In this step the information assets will be classified on the basis of priority which is critical for the organization. The risk is also assessed to determine probable consequence that arises from breach or leakage of information from CP and users platform. JGB is associated with these assets as owner of information asset so that the liability arising out of any breach can be easily adjudicated and managed. Risk assessment carried by CP will be shared and evaluated by JGB. This will create the post counter measures to enable security. One of the important aspects is risk assessment of malicious code run on PaaS and IaaS layers. The boundaries are created and assessed by JGB for inclusion into the security policy

C. Asset Management

The risk management is followed by asset management. The information asset is classified according to priority and labeled accordingly. JGB becomes the owner of asset equally responsible for any breach. The classification of information asset is an important step that will further devise the rules for application of security controls and intellectual property protection. The information will be classified into low, moderate and critical. The baseline security controls are also classified accordingly to protect the information asset. The classification and security controls of the information asset is documented and forwarded to JGB for approval as major part of security policy. The process is equally performed on the information asset, in all the layers SaaS, PaaS and IaaS.

D. Selection of Layers

The selection of layer is based on classification of information asset. The user will decide what type of services he is likely to have. This is determined keeping the risk assessment of CP, classification of asset and trust. JGB is developed to boost trust and coordinate the relationship between user and CP. SaaS is the most feasible state that can be accepted by the user. However, business process re-engineering needs to be aligned with technical support; it needs a layer where software can be customized for optimized performance. The selection determines security controls to be applied. The security controls decided during the asset management are coordinated with JGB for approval to be included in list of security controls while implementing the security policy

E. Security Policy

Considering the user risk assessment, asset classification and controls, determination of cloud layers, JGB will determine the security policy essential to implement the security controls and devise a strategy for its awareness. The board jointly determines technical security controls on the physical and logical level. The technical security control is dependent on the cloud layer which is used by cloud user. However, security controls are first generalized as baseline controls that can be applied to mitigate the risks for example applying access controls, configuration of firewalls, provisioning and deprovisioning etc. The main purpose is to create an awareness program for user who is adopting cloud and how his assets are protected, neutralizing mistrust for better governance. JGB sends the security policy for approval to enterprise management in order to sustain its alignment with corporate strategy.

F. Application of Security Controls

JGB approves the security policy and governs to be implemented in true spirit. The technical security controls are applied on the layer used by the user accordingly. These controls are applied distinctively on each layer which is currently used by cloud user.

G. Monitoring

CP will devise a program for systematic monitoring and evaluation of security controls to ensure baseline standards of quality are met. Quality evaluation and acceptance criteria for information systems, upgrades, and new versions shall be established, documented by the JGB with the approval of user. All the users under the enterprise control will be monitored and audit logs will be maintained. The audits logs will be reviewed by JGB. Any security incident will be reported to JGB for action to maintain the trust between entities and assess the maturity level of the CP.

H. Compliance and Audit

JGB is instituted to comply with local laws where the data or subject matter resides. The main intention of JGB is to harmonize the legal and jurisdictional difficulties to thwart the effect created by the gap. CP will provide the detailed relevant local laws that need to be complied by him and user to JGB. The board will formulate the policy and actions that are needed to abide by the local laws. This includes civil,

criminal, tort and corporate laws. The procedures agreed will be documented and user will be given full awareness of consequence of any breach of law.

The periodical security audits are essential to assess the security controls of CP, therefore Independent reviews and assessments shall be performed periodically to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements. The audits will include internal, external audits, vulnerability testing and penetration testing to ensure the security perimeters are in place. The responsibility of audit belongs to CP who will prepare procedure and plans to accomplish it. The procedures and plan will be reported to JGB for approval and subsequently the audit report will follow it. This will aware user about the CP internal and external controls security health.

I. Discussion and Evaluation

The governance framework is evaluated using structured approached, divided into three dimensions; the international security standards, law and evaluation by companies. The components of framework are derived from IT governance controls present in security standards. Though, cloud computing takes a new approach of business, the derivation of the framework modules were inevitably necessary because these existing standards matured and known as to implement best practices. Secondly, these standards have been developed over time improving its capability to secure information and certifying companies to an assurance level of maturity.

The second approach was consideration of law. Business and IT is widely accepted paradigm, however law has been always ignored on the grounds of its being rigid. Cloud computing is transnational, it attracts jurisdictional as well as assurance issues. The law defines the limitations, legal actions and provides measured control to sustain a governance environment. Some of the legal "controls" have been integrated into standards. For example COBIT is known as SOX compliant. Similarly, framework needs to evaluate under law. JGB is important both are corporate law or financial acts that maintain responsibility to be associated with responsible persons. For example SOX clearly state that financial statement is required to be attested by designated person. Similar laws are available in other countries which are not restricted to financial laws. Even the privacy laws of various countries validate components of framework. Therefore, framework life cycle and its modules needed to be evaluated through legal principles. The JGB was developed to solve the issue of legal jurisdiction, dispute resolution; SOX section 302, requirement by ISO27002 controls 6.1.1, 6.1.2, 7.1, 7.1.2 and other standards; there must be a responsible board for security governance. The JGB is main governance initiative capable of resolving issues that are currently retarding the adoption of the cloud. Similarly, other components were modeled. The third evaluation was conducted by sending the framework to companies. The companies gave the feedback that framework is applicable on PaaS and IaaS layers and not suitable for SaaS layer. However, JGB solves major issues that often arise out during the implementation. It was quite positive as the companies disclosed that they have marketing and support teams in place to solve issues of the cloud user but as far as cases of dispute resolution or SOX has not been witnessed. Legally, framework solves the issues of jurisdiction, responsibility and due care. Parallel to these, the framework has some limitations it has not been assessed for high risk countries. The evaluation is based on countries which has similar legal system based on common law and observe the principles of rule of law. These countries also practice good security practices and follow general rules laid down by international security standards and respect law of different countries. During the research and evaluation, USA, UK, Canada, Australia and New Zealand were chosen as low risk countries. The framework presented in the paper needs more evaluation for its iterative development and form a governance life cycle to be applied generally.

V. CONCLUSION

The paper presented a governance framework that addresses security in PCC. The process in the framework is iterative and needs to be updated whenever new advancement comes in any of three domains. The framework gives an emergent action to mitigate risks and improve security, governance and assurance within PCC. It decreases the gap between enterprises and CP moving them on joint platform to easily use it as a service for their business. The triangulation of standards, law and cloud layers is used to fill the gap and add extra security and assurance that can benefit user. It has some limitations in terms of acceptance of statutory laws of different country; framework solves this problem using JGB. The main aim of JGB is to harmonize the security requirements according to baseline security controls that can effectively protect the asset. JGB also signifies coalition of two entities on one platform to accept responsibility of business layer such as legal compliance to SOX, HIPAA, and GLBA etc. The motivation behind JGB was Globalization and legal precedents from case law of different countries that have ensured justice despite distance was a challenge. PCC is still under development and needs more maturity over time. The economic needs of society have often developed strategy to overcome obstacles, cloud computing is one of the emergent economic trends which are under study to evaporate the effects of costly technology system supporting enterprises. The future work is to develop the model with qualitative data from the consumer to balance the governance equation and automate digital contracts with assurance clauses from legal, security controls and business processes. Currently there are many organizations working to solve the issues in PCC. This work

is one small step to introduce a framework that is necessary to manage control, authority and governance to maintain security to protect user's data.

REFERENCES

[1] C. Ciborra, "Bricolage," in *The Labyryinths of Information*, ed: Oxford University Press, 2002, pp. pp 29-53.

[2] J. Voas and J. Zhang, "Cloud Computing: New Wine or Just a New Bottle?," *IT Professional,* vol. 11, pp. 15-17, 2009.

[3] H. Brian, "Cloud computing," *Commun. ACM,* vol. 51, pp. 9-11, 2008.

[4] I. Foster*, et al.*, "Cloud Computing and Grid Computing 360-Degree Compared," in *Grid Computing Environments Workshop, 2008. GCE '08*, 2008, pp. 1-10.

[5] L. Geng*, et al.*, "Cloud Computing: IT as a Service," *IT Professional,* vol. 11, pp. 10-13, 2009.

[6] M. Lijun*, et al.*, "A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues," in *Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE*, 2008, pp. 464-469.

[7] Salesforce.com. (2009, 9 july 2010). *what is cloud computing*. Available: http://www.salesforce.com/cloudcomputing/

[8] U. ISACA. (2010, 11 march 2010). *ISACA US IT Risk/Reward Barometer Survey*. Available: http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/ISACA-US-IT-Risk-Reward-Barometer-Survey.aspx?PF=1

[9] D. S. A. Allie Young, Gianluca Tramacere. (2008-2009, 11 july 2009). *User Survey Analysis: Economic Pressures Drive Cost-Oriented Outsourcing, Worldwide, 2008-2009*. Available: http://www.gartner.com/DisplayDocument?id=1057314

[10] B. R. Kandukuri*, et al.*, "Cloud Security Issues," in *Services Computing, 2009. SCC '09. IEEE International Conference on*, 2009, pp. 517-520.

[11] Dave Cullinane*, et al.* (2009, Security Guidance for Critical Areas of Focus in Cloud Computing. 84. Available: http://www.cloudsecurityalliance.org/csaguide.pdf

[12] ISACA and C. S. Alliance. (2009, 3 march 2010). *Cloud Computing: Business BenefitsvWith Security, Governance and Assurance Perspectives*. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf

[13] ENISA. (2009). *Cloud Computing Risk Assessment*. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[14] L. M. Kaufman, "Data Security in the World of Cloud Computing," *Security & Privacy, IEEE,* vol. 7, pp. 61-64, 2009.

[15] A. M. Kjaer, *Governance, Key concepts*, 1 ed.: Wiley, John & Sons, 2004.

[16] J. N. Rosenau, *Governance in the Twenty First century* vol. 1, 1995.

[17] P. Weill and J. Ross, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*: Harvard Business School Press, 2004.

[18] K. Na-yun*, et al.*, "SOX Act and IT Security Governance," in *Ubiquitous Multimedia Computing, 2008. UMC '08. International Symposium on*, 2008, pp. 218-221.

[19] S. Sahibudin*, et al.*, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," in *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, 2008, pp. 749-753.

[20] D. S. Barnhill, "CLOUD COMPUTING AND STORED COMMUNICATIONS: ANOTHER LOOK AT QUON V. ARCH WIRELESS," *Berkeley Technology Law Journal,* vol. 25, 2010.

[21] J. Dean, "Enterprise Software as Service," *Queue,* vol. 3, pp. 36-42, 2005.

[22] C. C. David and Y. C. Amy, "Analysis of a new information systems outsourcing practice; software as a service business model," *Int. J. Inf. Syst. Chang. Manage.,* vol. 2, pp. 392-405, 2007.

[23] A. Stefan*, et al.*, "Multi-tenant databases for software as a service: schema-mapping techniques," presented at the Proceedings of the 2008 ACM SIGMOD international conference on Management of data, Vancouver, Canada, 2008.

[24] Thomas Ristenpart*, et al.*, "Hey, You, Get Off of my Cloud: Exploring information Leakage in the Third Party Compute Clouds," presented at the CCS'09, ACM, Chicago, Illinois, 2009.

[25] CSA. (2010, 19 august 2010). *controls matrix*. Available: http://www.cloudsecurityalliance.org/Research.html

[26] *Personal Information Protection and Electronic Documents Act*, 1983.

[27] *Data Protection Act*, 1998.

[28] *Regulation of Investigatory Powers Act*, 2000.

[29] P. Balboni, "Data Protection and Data Security Issues Related to Cloud Computing in the EU," *ISSE 2010 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe Conference 2010,* 2010.

[30] T. R. Gubins, "Warshak v. United States: The Katz for Electronic Communication," *Berkeley Technology Law Journal, Forthcoming*.

[31] P. Wang, "CHASING THE HOTTEST IT: EFFECTS OF INFORMATION TECHNOLOGY FASHION ON ORGANIZATIONS," *MIS Quarterly,* vol. 34, p. 63, 2010.

[32] S. Bradshaw*, et al.*, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services," *SSRN eLibrary*.

[33] L. Poppo, and Zenger, T, "Do Formal Contracts and Relational Governance Function as Substitutes or Complements?," *Strategic Management Journal* vol. 23, pp. 707-725, 2002.