TRIANGULATION THEORY: AN APPROACH TO MITIGATE GOVERNANCE RISKS IN CLOUDS

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

Lech Janczewski
Dept of Information Systems and Operational Management, Business School,
University of Auckland
Auckland, New Zealand
lech@auckland.ac.nz

Abstract

Cloud computing is a business concept that delivers technology "as a service". Its lower cost of operation is the main economic driver for consumers and enterprises. The major obstruction to its adoption is security and governance risks inherent in its transnational nature. These risks are associated with relative change of governance level within the cloud service layers during the relationship between the customer and cloud provider in public cloud computing (PCC). The responsibility and authority of both the entities differs in each layer bifurcating influence of due care and due diligence. The existing internationally recognized security standards International Organization for Standardization (ISO 27001/2), Control Objectives for Information and Related Technology (*COBIT*) *etc do not handle cloud computing domains from every aspect. Similarly, due to transnational nature of PCC, legislative acts of one country cannot get dejure recognition in different jurisdiction. These variations incapacitate PCC from achieving assurance and governance level to sustain cloud security. The paper will present a theoretical model to develop common criteria using triangulation of service layers, security standards and statutory laws, essential to maintain governance and security.*

Keywords-*Governance, Cloud Computing, Security, Assurance*

1 INTRODUCTION

Today, it is humanly impossible to run our lives without connection oriented[1, 2] services of IT. Majority of actors holding smart phones reflect inevitable importance of connectivity that provide financial and business services. The actors unconsciously trust these technological services despite the fact; they do not know where the data is choreographed and maintained. Historically, such services has been around for more than a decade, it gained impetus and recognition as cloud computing [3] since last few years.

Cloud computing is "as a Service"[4, 5] model. The services are provided by cloud provider in the form of software and hardware resources. The cloud user does not invest money to buy IT infrastructure but rents services from cloud provider. It is cost effective, saves money on IT infrastructure, promises rapid allocation of resources and on demand provisioning[6]. It creates an environment that has no conflicts with and within the organization[7]. Information Systems Audit and Control Association (ISACA) survey asserts that enterprises are embracing cloud computing for outsourcing management of IT infrastructure, to cut IT cost [8] and commonly accepted paradigm by executives[9]. These existing advantages of cloud computing does not absolve it from inherent security risks[10, 11] which outweigh benefits[8]. Cloud security alliance (CSA) has identified security risks in thirteen different domains of cloud computing and emphasize enterprise to adopt cloud services with precaution[12]. Same has been voiced by security communities[10, 13, 14] and government[15].

Cloud computing is a naturally occurring bricolage[16], an innovation that stems from existing technological means. There are various definitions [4-6, 17, 18] of cloud computing, however the definition of National Institute of Standards and Technology (NIST)[19] is widely accepted.. NIST divides cloud computing into three layers; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). NIST defines cloud computing 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*"*
The definition is simple and elaborates the key aspects of the cloud computing. The definition is seminal work accepted by majority of companies.

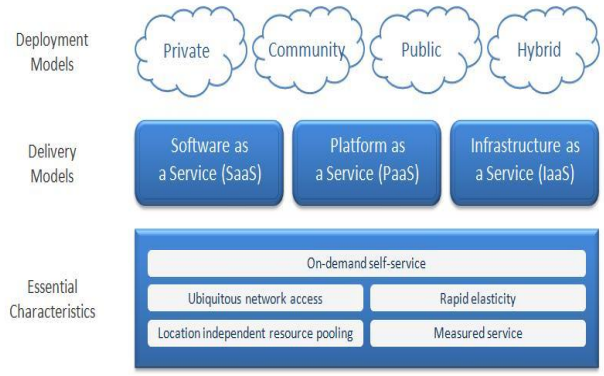

Figure 1: Cloud definition[19]

.

The major impediment to cloud adoption is grounded in the deployment models especially public cloud computing (PCC) where "the provider is transnational. European Network and Information Security Agency (ENISA) has reported jurisdictional security risks[13, 15]. Some sources predicted increase in cyber warfare[20] and intelligence espionage[15]. This paper argues that cloud computing is engagement between cloud user and cloud provider that requires set of governance rules to execute stable relationship and mitigate risks. The existing governance structure of PCC does not present a balanced governance constitution which can cause considerable security risks.

The section 2 will define governance that is used in research context followed by variation of governance within the cloud layers between customer and provider and section 3 will illustrate a theoretical model of governance with different rules that validate quality of governance for mitigation of risks followed by conclusion.

2 GOVERNANCE

Governance is a relative control that gives reliable assurance of trust and accountability. Governance has its origins from social sciences, latter the term is used in different factions of scholarship. Governance has its origins from Greek verb κυβερνάω [*kubernáo*] which means *to govern, steer, devise guide control[21]*.It was first used by Plato to design a system of rule. There are various definitions of governance found in corporate governance, IT governance, politics, economics, globalization and administration. The main concern of the paper involves IT, services and enterprise. It is important to look into the definition from different perspectives:-

Governance from IT perspective*:* IT governance literature defines governance as "is the 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" (ITIG).Weill et al defined IT governance is about specifying the decision rights and accountability standard to encourage desirable behavior in using IT[22]. IT governance is responsible for these two main functions; it delivers value to the business and mitigation of IT risks [23, 24]. The other definitions, governance is system of rules of power and control[25]. These definitions purports control, accountability, desirable behavior, mitigation of risks, return on investment, system of political rules and strategic decisions. The main objective of this paper is to develop an understanding of governance involving PCC. Therefore governance is taken in literal sense can be defined as "the governance of application, services and processes between the two main entities; user and provider, by creating a balance between the shared set of responsibilities and liabilities for better control and accountability to sustain governance".

.

2.1 Variation of Governance in Cloud layers

There are three layers of cloud, software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

SaaS is supported by the underlined layers of PaaS and IaaS. The user access the software interface using the web browser [26-28]. The services offered on this layer by different cloud providers are Business intelligence, Customer Relationship Management, Supplier Relationship Management and Human Resource Management[29]. The Table 1 shows governance variation and major control is with the cloud provider.

Table 1: Governance Level on the SaaS layer[13]

Governance Level	
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 software security
Authentication	Management of network security
	OS patch management
	Incident response and resiliency
	Monitoring and Maintenance
	Compliance with standards and legal regulation

PaaS layer gives developers to customize, develop and deploy cloud applications. The layer gives more power to user for managing his applications. Security level is decreased as compared to SaaS from provider perspective.

The deployment and testing of the application is the sole responsibility of the user. However, there is a possibility of running malicious code in this layer [30]. Table 2 illustrates the reduction of obligations of provider and shift of control towards the user. It increases his power to manage applications

Table 2: Governance Variation at PaaS[13]

Governance Level	
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	OS patch management
Testing of Software	Incident response and resiliency
Maintenance of software and software security	Monitoring and Maintenance
Compliance with law related to malicious software	Compliance with standards and legal regulation

IaaS is the lowest layer. It lays the security foundation at the cloud provider domain. The security decreases as the cloud provider gives more power to the consumer to enjoy the facilities by running applications and using virtual operating system.

Table 3: Governance level at IaaS layer[13]

Governance Level	
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	

Figure 2 illustrates table 1, 2 and 3 to show the change in security and control.

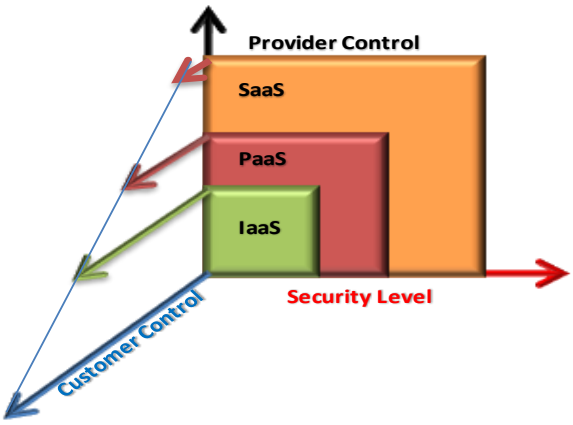

Figure 2: Security levels at cloud layers

The variation of control from cloud provider to user divides responsibility, control, authority and security. SaaS level shows minimum control by customer. It increases gradually to gain maximum aperture at IaaS level. These shifts create division responsibility between due care and due diligence. For example deploying software by user at PaaS turns out to be malicious. The initial responsibility to test application is of user, however, continuous due diligence controls are applied by provider. It originates a governance gap that who is responsible for what? Another aspect is ownership of software and hardware in cloud environment remains with cloud provider. In this state, the user data is exposed to surveillance, leakage and breach of intellectual property right. The absence of such governance and cross boarder flow of information diminishes the assurance, auditing, accountability and raises jurisdictional issues[13].

2.2 Existing Governance frameworks

The main aim of governance frameworks is to introduce the security best practices within the organization with the consent of board of directors [23, 24]. In this paper, cloud computing is analyzed under the lens of COBIT and ISO27001 considering governance as main discipline of research scholarship.

The figure 3 shows the qualitative analysis of frameworks. The data is taken from the CSA matrix[31]. The matrix show controls of ISO27002, COBIT, Health Insurance Portability and Accountability Act (HIPPA), National Institute of Standards and Technology (NIST SP800-53), Payment Card Industry Data Security Standard (PCI-DSS) and classify these controls according to the layers of cloud computing, provider and user. The qualitative analysis was performed to understand the governance control exercised by cloud user and provider.

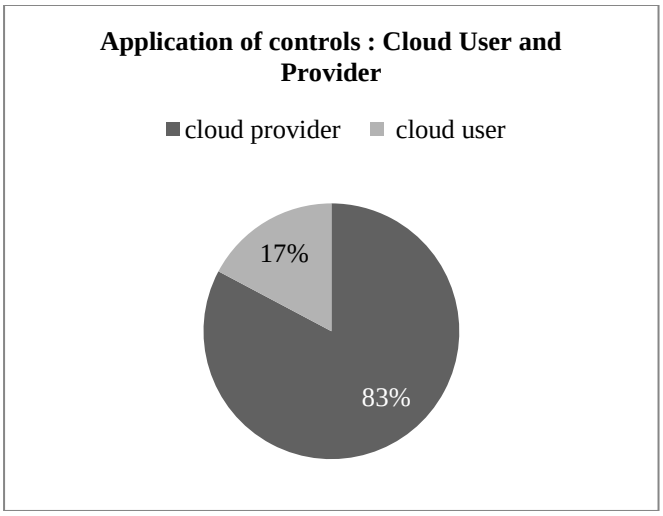

Figure 3: Degree of Control between Cloud user and Provider

These frameworks are designed to articulate security best practices in the organization. The implementation is effective because the organizations own the assets. Ownership and possession of assets leverages organizations to have absolute control and authority during implementation. The outsourced partnerships are carefully scrutinized while leveraging scarce control of authority to them to use organizational asset. Figure 3 shows the dominant control of the cloud provider. The conceptual model of cloud computing is not ownership based, but As a Service model. The information assets are ostensibly owned by the customer and running on the servers of cloud provider. The financial services running on PCC sometimes require compliance to local as well as transnational laws. For example For example Sarbanes-Oxley act 2002 (SOX) [23] has clauses that requires financial officer and chief executive to attest the accuracy of the financial reports[23], companies must assess its internal controls through rigorous auditing and implement the segregation of duties. Similarly there is Gramm-Leach-Bliley Financial Modernization Act (GLBA)**,** directs the financial institutions to ensure the security of customer information, protect against unauthorized accesses, privacy and preserve the integrity of the customer information assets. Similar provisions can be found in European Union(EU) directives, 4th Amendment of United States constitution, Canada[32], UK[33, 34], EU, 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 auditing and compliance to law can be merely impossible to be observed by cloud provider and user due to distance and jurisdictional state of PCC. Both entities may be in jurisdiction of different countries having differences in accepting the local and contractual laws.

2.3 Preliminary assumptions:Public Cloud

Considering the various literature and risks reports, the public cloud is re-defined to under umbrella of jurisprudence. The assumptions are taken to provide a constructive protection to both entities and mitigate the risks. The paper will have following assumptions:-

- Cloud provider and user both reside in the low risk country
- Both the countries have established the practice of good rule of law
- Accepted common grounds of law. For example choosing countries which accept common law or civil law
- Having good governance level

3 TRIANGULATION MODEL

Transnational nature of PCC involves three domains: Cloud service layers, IT security standards and statutory laws. These three domains need an alignment with each other to mitigate the security risks. The intersection surface in Figure 4 presents probable variables that can mitigate risks and secure both parties. The model covers the relationship of customer and provider from three angles, internal controls, 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. Once these rules of liability, internal controls and operational security is set and agreed between the cloud user and provider, it is expected to achieve assurance and security. It produces set of rules that are essential for governance of relationship between user and provider that can be further written as contractual agreement.

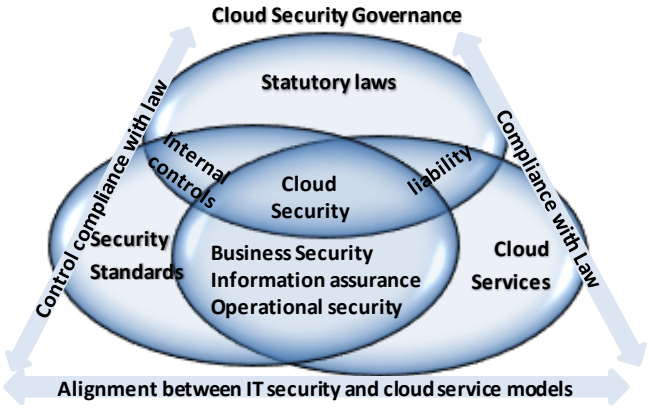

Figure 4: Triangulation method

Triangulation brings governance and assurance to the PCC. The word assurance means in the light of ISO-15408 as "Grounds for confidence that an entity meets its security objective". This can be assured by gathering the common accepted rules from three domains which produces cloud security. The horizontal assurance is alignment between IT security standards and cloud services models. The vertical alignment is achieved between law, cloud service layers and standards. The subsets of this alignment are operational security, liability and internal controls. The explanation of the entities is as follows:-

3.1 Operational Security

It is amalgamation of proactive and reactive security measures focused to ensure resilient operation of infrastructure and management of service levels. The major failures of the organizations are due to lack of understanding the operational security (OS) within the organization[29]. The operational security includes outsourcing, data protection, threats, security controls and contract management (CM). In OS, the first step is classification of information asset critical for business application under the lens of confidentiality, integrity and availability (CIA) with operational risk assessment. The information asset differs on each layer. Once the requirement engineering is done, information asset can be protected using the security controls specified for each layer of PCC. The business security and information assurance is dependent on operational security. This is evaluated by reliability and trustworthiness of the system

Table 4: Example of OS on SaaS layer

Governance Level			
User	**Cloud Provider**	**ISO27001**	**COBIT**
Risk Assessment	Risk Assessment	4.1, 4.2, 10.1.2, 10.2.3	PO 9.1 to 9.6
Asset Management	Asset Protection	7.1, 7.2	PO2
Access controls	Access Policy	11.1 to 11.7	DS5.3, DS5.11

The table 4 gives excerpt of controls as an example that can be applied to cloud user and provider at SaaS layer. For example asset management, at the SaaS layer, the software is provided by the provider. The application and hardware security is within the power of the provider. PO2 of COBIT states that the enterprise must have an enterprise information architecture model, data dictionary, classification of information asset and strategy to maintain the integrity. Similarly ISO27002 have almost same clauses. The only difference between the clauses of these two standards is ISO27002 states the ownership of assets, where as COBIT adds process ownership for maturity evaluation. Process ownership[35] enables compensation, liability and benefits while outlining acceptance of shared risks. These common themes of standards must be taken as best practices to ensure common grounds of an accepted policy of operational security by both parties. The knowledge emerging from these grounds may also be sustained as partnership agreement. These variables can be increased with the maturity of relationship to give more protection. Further these controls can be written in service level agreements (SLAs) to enforce set of policies to execute governance.

3.2 Liability

The three cloud service layers use, process, communicate and retain valuable consumer data in the form of information asset. The breach associated with information asset, effects Company's business reputation, trust and compromises its security. It incurs liability on the entity and results in legal action against the party which has committed the breach. The PCC has two issues, one is it is transnational and other is shift of liability within the layers during the amount of control practiced by the cloud user and provider. Liability varies in terms of due care and due diligence in each layer. The liability can be distinctively applied in three domains of cloud service, SaaS, PaaS and IaaS. The action that arises from breach can be in the form of torts, claim for damages and statutory fine.

Table 5: Description of variables for statutory protection for liability

	Liability on Layers		
	Cloud user	Provider	Action
SaaS		Breach of data protection, privacy	Tort, data protection laws, cyber crime laws, Forensic laws, Contractual Obligations etc
PaaS	Testing and Malicious code , breach of data	Intrusion detection/prevention systems, firewalls, Insider attack	
IaaS	Malicious code, leakage, vulnerability in software	Physical and software controls of data protection	

Table 5 only gives the synopsis of legal literature. For example cloud provider is providing the financial services to the cloud user, the liability of data protection will be on the cloud provider. If the breach or leakage of data occurs, according to data protection act 1998 of UK, the cloud provider residing in UK can be fined for 500,000 pounds. Similarly grievance from data breach can be approached using tort in United States, privacy and data protection acts of various countries. The other important factors while considering the liability is to understand whether the law of cloud provider country can provide assurance and

accountability. It is therefore imperative to consider following mandatory options:-

- The countries of both cloud user and provider have reached a good governance level in terms of socio-political aspect;
- Both countries respect and judiciously practice rule of law;
- The statutory acts of both countries correlate with each other for example based on common law paradigm like USA, UK, Australia, New Zealand;
- Cloud provider and user reside in low risk country;
- Judicial decisions are accepted by both the countries

The law will provide assurance for data protection if found on the common grounds. If there are new enactments and provision of law accepted by both the parties, it will become a consideration of contract. For example if the cloud provider is in UK and cloud user is in Australia, cloud user can ask for data protection under data protection act 1998 of UK. It will grant user to claim damages that may not be possible while using Australian law. This emerging provision can become part of agreement where both parties are agreeing on the same grounds. It also signifies alignment of service layers with the statutory law.

3.2 Internal Controls

The major accounting scandals WorldCom, Enron and Tyco have shown accountants inability to proactively audit the weak controls. The frauds of such magnitude led to the promulgation of laws that provide guidance for integrity of the internal controls. Committee of Sponsoring Organization (COSO) defines internal controls to provide reasonable assurance to achieve following objectives[23]:-

- Efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The majority security standards have the clauses that strictly require the compliance of statutory laws but do not verify outsourced data running on the internal controls of cloud provider. The financial data of user running on the provider cloud requires assurance, internal assessment and attestation. SOX direct the financial companies to verify, attest and disclose financial reports. It also penalizes company for intentional alteration of records under section 802. The international standards ISO27001, COBIT, COSO, all require the compliance and strict adherence to laws. The main concern is the common ground for implementation of the processes. The cloud user and provider need to agree on common terms to ensure integrity of internal controls. For example cloud provider is in USA and user resides in Australia, they both must agree either on SOX or Corporate Law Economic Reform Program (CLERP) Act 2004 of Australia. The transnational compliance of law may be documented for dispute resolution, auditing, accountability, performance of the contract and liability. Procedures to maintain the financial data at the provider end can be formalized by both entities on common grounds especially to preserve its integrity.

3.4 Alignment

The security standard, cloud services and transnational laws needs to be aligned together to maintain effective control of governance and cloud security. The subsets operational security, liability and internal controls are the iterative procedures, policies, direction based on agreed common criteria to engage obligations among two entities. Figure 4 shows the general concept of alignment focused on three main domains. The alignment is achieved horizontally and vertically, using alliance between two cloud provider and user. Figure 5 is subset of figure 4, underlines the requirements engineering within OS, internal controls and liability.

During the implementation of OS, the cloud user and provider use existing security best practices to implement security controls. The emergent controls are extended controls which are outcome of classification of controls from different standards and agreed between two entities. These controls will add more security. Similarly, liability is shared using existing protection of law and balanced by the emergent legal acts or precedents acceptable to both entities. The integrity of internal controls are maintained in the same criteria using the existing procedures of law and fortified by emergent procedures demanded by transnational laws. The emergent knowledge is based on common criteria for unified processing.

The two knowledge bases, existing and emergent from triangulation of subsets provides set of obligations and assurance criteria. These obligations and assurances are documented in form of Service Level Agreements (SLAs) and contracts to reinforce the set of governance rules to sustain the information assurance, business and operational security. It can be implemented as a software agent that can handle the legal contracts and monitor it for the record of both the entities. The process is iterative and obligatory improvements can be enhanced. This relationship can be assessed using stages of capability maturity model of COBIT.

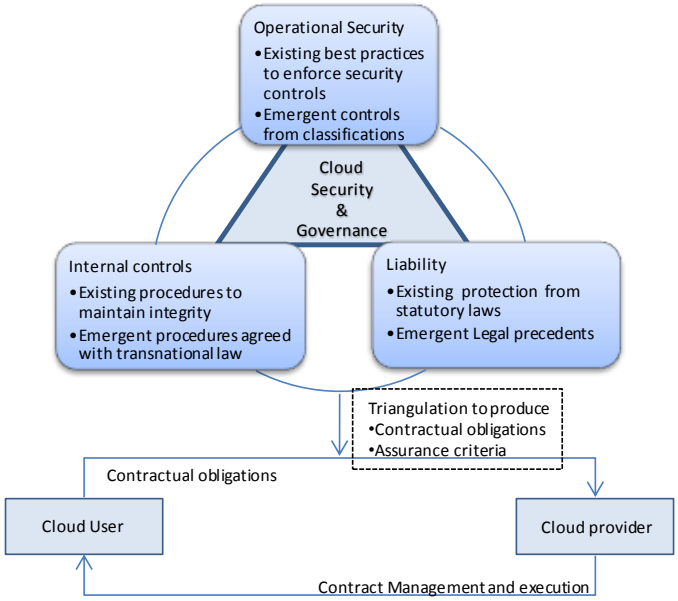

Figure 5: Triangulation outcome

4 CONCLUSION

The paper presented triangulation model to fortify the security aspects in PCC. The globalization is in the process and recognition of law, international standards are progressively accepted. The security and governance assurance of PCC will allow consumers and enterprises to easily use it as a service for their business. The triangulation method is a way for adding extra security and assurance for benefit of consumers. It has some limitations in terms of acceptance of statutory laws of different country. There have been cases where precedents from different countries have been cited to ensure justice. The model is part of current research study. The three mitigating factors were research through the statutory laws, cloud computing literature and security standards. 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. The solution can be only possible if these three domains are aligned to produce security and governance. Cloud computing is still developing and currently there are many organizations working to solve security issues. In future, there will be solutions like information assurance criteria to minimize risks and attest information assets in the clouds.

References

[1] T. Peter, *et al.*, "Roomware-Moving Toward Ubiquitous Computers," *IEEE Micro*, vol. 22, pp. 36-47, 2002.

[2] M. J. Leonard and R. Daniel, "The relevance of social issues in ubiquitous computing environments," *Commun. ACM*, vol. 45, pp. 88-91, 2002.

[3] Cnet News, "What is cloud computing? interview with Kevin Marks Google," ed, 2008.

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

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

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

[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] New Zealand Government. (2010, *Governance Management and Project Risk*. Available: http://www.e.govt.nz/policy/trust-and-security/government-use-of-offshore-ict-service-providers/governance-management-project-risks

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

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

[18] 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.

[19] P. Mell. (2009, march). *NIST Definition of cloud computing*. Available: http://csrc.nist.gov/groups/SNS/cloud-computing/

[20] McAfee. (2009, *Virtual Crminology report 2009*. Available: http://resources.mcafee.com/content/NACriminologyReport2009NF

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

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

[23] 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.

[24] 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.

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

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

[27] 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.

[28] 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.

[29] A. Chris, *et al.*, *IBM REDBOOK :Multitenant Utility Computing on IBM Power Systems Running AIX*: IBM, 2009.

[30] 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.

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

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

[33] *Data Protection Act*, 1998.

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

[35] M. H. Larsen and R. Klischewski, "Process ownership challenges in IT-enabled transformation of interorganizational business processes," in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 2004, p. 11 pp.