# Compliance and Data Sovereignty Issues on Cloud Technology

Vignesh Palanisamy
Student
Eastern Institute Of Technology
Napier, New Zealand
**palanv1@student.eit.ac.nz**

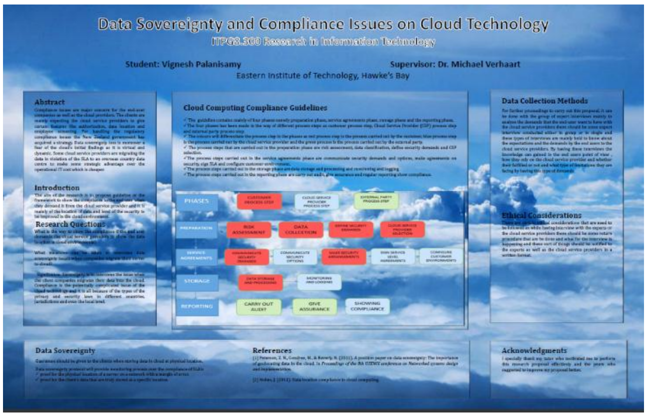
Michael Verhaart
Supervisor
Eastern Institute Of Technology
Napier, New Zealand
**mverhaart@eit.ac.nz**

## ABSTRACT

Compliance issues are a major concern for the end-user companies as well as the cloud providers. Clients are expecting the cloud service providers to give certain features like authorization, data location and employee screening. For handling the regulatory compliance issues the New Zealand government has acquired a strategy. Data sovereignty loss is moreover a fear of the cloud's initial findings as it is virtual and dynamic. Some cloud service providers are migrating the data in violation of the Service Level Agreements (SLA) to an overseas country data centre to make some strategic advantage over the operational IT cost which is cheaper. The data sovereignty protocol will provide monitoring process over the compliance of SLA's. SMX a cloud hosting company states the issue of the data sovereignty is starting to drive business decision making closely connected to the data that are stored in the cloud.

## Keywords

Data sovereignty, compliance, SLA, SMX.



Data Sovereignty and Compliance Issues on Cloud Technology
ITPG8.300 Research in Information Technology

Student: Vignesh Palanisamy
Supervisor: Dr. Michael Verhaart
Eastern Institute of Technology, Hawke's Bay

Abstract

Introduction

Research Questions

Cloud Computing Compliance Guidelines

PHASES
CUSTOMER PROCESS STEP
CLOUD SERVICE PROVIDER PROCESS STEP
EXTERNAL PARTY PROCESS STEP
PREPARATION
RISK ASSESSMENT
DATA COLLECTION
DEFINE SECURITY DEMANDS
CLOUD SERVICE PROVIDER SELECTION
SERVICE AGREEMENTS
COMMUNICATE SECURITY DEMANDS
COMMUNICATE SECURITY OPTIONS
MAKE SECURITY ARRANGEMENTS
SIGN SERVICE LEVEL AGREEMENTS
CONFIGURE CUSTOMER ENVIRONMENTS
STORAGE
DATA STORAGE AND PROCESSING
MONITORING AND LOGGING
REPORTING
CARRY OUT AUDIT
GIVE ASSURANCE
SHOWING COMPLIANCE

Data Collection Methods

Ethical Considerations

Data Sovereignty

References

Acknowledgments

## 1. INTRODUCTION

The aim of the research is to develop a guideline or framework to show the compliance to the end user when they ask it from the cloud service provider and it is mainly of the location of data and level of the security to be improved in the cloud environment. Another thing the proposal mainly deals with is the data sovereignty issue and for that a data sovereignty protocol is to be proposed and by following certain companies how they are solving the issues while they migrating the sever and the data to the cloud a necessary and acceptable solution need to be proposed for sorting out these issues as the end users are facing in this process.

## 2. RESEARCH QUESTIONS

What is the way to show the compliance if the end user demands the cloud service providers to show the data location in cloud environments?
What measures can be taken to overcome data sovereignty issues when companies migrate their server to cloud?

At first the question regarding the compliance is framed as what the level Service Level Agreement (SLA) need to be signed so between the end users and the cloud service providers. But the issue mainly regarding the compliance is the location of the data that can't be seen by the end user and so if the end user demands to show the compliance how the cloud service provider will show it. The question regarding the data sovereignty is to overcome the issue when the client companies migrates their data into the cloud.

## 3. LITERATURE REVIEW

In a cloud environment the complexity of the security risk can be seen by analysing its deployment models and the delivery models. The cloud is being deployed by the ways of public cloud, private cloud, hybrid cloud and the community cloud (Subashini, & Kavitha, 2011). When looking at all the fundamental service delivery models SaaS is the most concerned model in security as it has less control over the security (Hashizume, Rosado, Fernández-Medina & Fernandez, 2013).

There are some legal regulations for the companies to follow if they transfer some sensitive data and as well as the cloud service providers used to hide the locations in which the data are stored to prevent from the physical attacks and there should be some security mechanisms that are to be followed to prevent from the risk factors (Martens & Teuteberg, 2011).

The government of New Zealand exhibited some ambivalence in the perspective of regulatory compliance towards cloud computing technology. The government of New Zealand also stated support and confidence in the field of cloud computing through the Department of Internal Affairs, which describe a

This poster paper appeared at ITX 2014, incorporating the 5th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2014) and the 27th Annual Conference of the National Advisory Committee on Computing Qualifications, Auckland, New Zealand, October 8-10, 2014. Mike Lopez and Michael Verhaart, (Eds).

change towards the use of cloud computing as one of its current priorities for government information and communications technology (Matsurra, 2011). The sovereignty and the privacy of the data may differ from one jurisdiction to another and bringing down some of the legal obligations to the company which should protect the end-users data (Vaile, Kalinich, Fair & Lawrence, 2013).

## 4. THEORETICAL PERSPECTIVES

SLA@SOI framework is the framework that is used develop its own infrastructure to manage and deploy virtual machines. SLA@SOI framework is also providing an SLA management framework that provides support to the service level objectives. XACML framework is another framework for implementing the compliance and while doing it the framework assembles a technical infrastructure that is already existing.

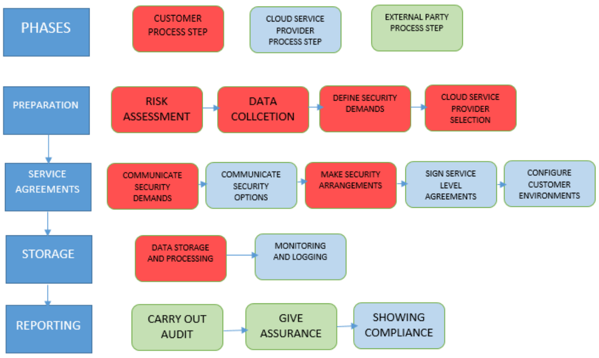

PHASES
CUSTOMER PROCESS STEP
CLOUD SERVICE PROVIDER PROCESS STEP
EXTERNAL PARTY PROCESS STEP
PREPARATION
RISK ASSESSMENT
DATA COLLCETION
DEFINE SECURITY DEMANDS
CLOUD SERVICE PROVIDER SELECTION
SERVICE AGREEMENTS
COMMUNICATE SECURITY DEMANDS
COMMUNICATE SECURITY OPTIONS
MAKE SECURITY ARRANGEMENTS
SIGN SERVICE LEVEL AGREEMENTS
CONFIGURE CUSTOMER ENVIRONMENTS
STORAGE
DATA STORAGE AND PROCESSING
MONITORING AND LOGGING
REPORTING
CARRY OUT AUDIT
GIVE ASSURANCE
SHOWING COMPLIANCE

Figure 1: Guideline for Cloud Computing Compliance (Noltes, 2011)

The guideline (Figure 1) consists of four phases namely preparation phase, service agreements phase, storage phase and the reporting phase. The four phases have been made in the way of different process steps as customer process step, Cloud Service Provider (CSP) process step and external party process step. The colours will differentiate the process step in the phases as red process step is the process carried out by the customer, blue process step is the process carried out by the cloud service provider and the green process is the process carried out by the external party.

The process steps that are carried out in the preparation phase are risk assessment, data classification, define security demands and CSP selection. The process steps carried out in the service agreements phase are communicate security demands and options, make agreements on security, sign SLA and configure customer environment. The process steps carried out in the storage phase are data storage and processing and monitoring and logging. The process steps carried out in the reporting phase are carry out audit, give assurance and regular reporting show compliance (Noltes, 2011).

## 5. RESEARCH METHODS

To carry out this research, it is envisaged to conduct expert interviews mainly to analyse the demands that the end-user wants to have with the cloud service providers there should be some expert interview conducted either in group or in single and these types of interviews are mainly held to know about the expectations and the demands by the end users to the cloud service providers. By having these interviews the knowledge can gained in the end users point of view , how they rely on the cloud service provider and whether their fulfilled or not and what type of limitations they are facing by having this type of demands (Noltes, 2011).

## 6. ETHICAL CONSIDERATIONS

There are certain ethical considerations that are need to be followed as while having interview with the experts or the cloud service providers there should be some return procedure that are be done and what for the interview is happening and these sort of things should be notified to the experts as well as the cloud service providers in a written format. During the interview the confidentiality is more important and the while having the expert interviews the form of data that are gained from the experts either a tape recording or writing should always under the permission of the experts should give assent in the written form.

## 8. REFERENCES

[1] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 1-13.

[2] Martens, B., & Teuteberg, F. (2011). Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model. In *AMCIS*.

[3] Matsurra, J. (2011). Opinion: Regulatory compliance in the cloud. Retrieved from http://www.computerworld.co.nz/article/497303/opinion_regulatory_compliance_cloud/

[4] Noltes, J. (2011). Data location compliance in cloud computing.

[5] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11.

[6] Vaile, D., Kalinich, K., Fair, P., & Lawrence, A. (2013). Data Sovereignty and the Cloud–A CIO’s Guide.

.