A New Cloud Computing Governance Framework

Ahmed Shaker Saidah and Nashwa Abdelbaki
School of Information and Communication Technology, Center for Informatics Science, Nile University, Cairo, Egypt
ahmed.shaker@nileu.edu.eg, nabdelbaki@nileuniversity.edu.eg

Keywords: Security Framework, Governance Model, Cloud Computing.

Abstract: Nowadays, most service providers adopt Cloud Computing technology. Moving to Cloud creates new risks and challenges. The Cloud era is to outsource our services to Cloud Service Provider (CSP). However, we have to develop a strong governance framework to review the service level, to manage risk effectively and to certify that our critical information is secure. In this paper, we develop an innovative governance model. It is based on the theoretical Guo, Z., Song, M. and Song, J governance model for Cloud computing. We distribute Cloud Control Matrix (CCM) on the Guo's model categories. This turns the theoretical Guo's model to a practical model. Governance model alone will not allow us to bridge the gap between control requirements, technical issues and business risks. As a result, we introduce a new Cloud governance framework using the processes on the new Cloud governance model.

1 INTRODUCTION

Cloud Computing is a new term for an old service with new features. Many of us used to have an e-mail account during the last two decades. Data location, storage and processing are usually unknown to the user. In fact, this was a kind of Cloud service. Cloud was known as on demand infrastructure in the 90s and as Grid/Utility computing in the 2000s. Clouds and Grids are common in their vision, architecture and technology, but they differ in security, programming model, business model, compute model, data model and applications (Foster and Zhao et al., 2008, pp. 1-10). Earlier in these days, it was too risky to store our data outside organization premises; safety was a concern.

Data is the most valuable asset in any organization. It can be categorized as PI (personal information) or organizations' data. Nowadays, all internet users intensively process and store data on the Cloud. Cloud Computing depends on sharing of resources to gain economies of scale. It focuses on maximizing the effectiveness of the shared resources. Despite the benefits promised by Cloud computing, we see that essential improvement on technologies and operations governance are needed to enable widely adoption of Cloud services (Popovic and Hocenski, 2010, pp. 344-349). The best way to protect data outside organizationpremises is to define a policy to organize the relation between the owner and service provider. Policy definition requires well-developed information security governance framework (Borgman and Bahli et al., 2013, pp. 4425-4435).

It is mandatory for any organization to follow a framework for establishing information security governance environment. The framework will be utilized by the business across the organization (Mukherjee and Sahoo, 2010, pp. 31-34). We create a new Cloud governance framework for helping organization to govern the Cloud services. It is a measurable, sustainable, continually improving and cost effective framework on an ongoing basis (Li and Zhou et al., 2010, pp. 2843-2848) (Ahmad and Janczewski, 2011, pp. 372-379).

The rest of this paper is organized into six sections. Section II discusses related works in governance and Cloud computing. We will go through existing Guo's Model and show the gap between its theoretical model and practical world, and will go through the pros and cons of the model. We propose our new Cloud Computing definition in section III. Section IV illustrates our proposed new model of Cloud Governance. Our new governance framework is introduced in section V. Finally, conclusion and future work are presented in section VI.

2 RELATED WORK

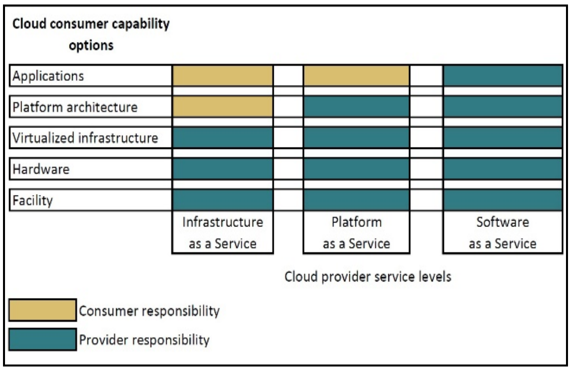
Cloud Computing is a relatively new term in the computing world. The definition of Cloud Computing from NIST (2009) is very common and almost all other definitions are part of this definition (Mell and Grance, 2011).

Cloud Computing becomes a huge market. Relations between services inside the Cloud are complicated. Virtualization vendors use different APIs. This creates many obstacles and challenges when moving between Clouds. Infrastructure inside the Cloud contains many layers of shared resources. Software licensing and end users license and agreement have many parameters and stages (Li and Chinneck et al., 2009, pp. 33-40). Federations and access control between service provider premises and end user premises become vague (Copie and Fortis et al., 2013, pp. 1229-1234).

The Cloud services become a self-service through websites. Customers can customize orders by themselves, which mean that they need to access the Cloud via all connectivity facilities. The user can increase or decrease the usage of the resources that is distributed across all provider premises.

Cloud Computing service models (SaaS, PaaS, IaaS) can be deployed in public, private or mixed model. User Control is varying from model to other and increasing or decreasing depending on the features and capabilities provided by the service provider or needed by the customer, (Figure 1) (*NIST Cloud Computing Security Reference Architecture*, 2012).

In SaaS model as an example, the Cloud user accesses the web service through any type of connectivity via web browsers, and he does not have control to the infrastructure or applications running in the Cloud.



Cloud consumer capability options	Infrastructure as a Service	Platform as a Service	Software as a Service
Applications	🟨	🟨	🟦
Platform architecture	🟨	🟦	🟦
Virtualized infrastructure	🟦	🟦	🟦
Hardware	🟦	🟦	🟦
Facility	🟦	🟦	🟦

Cloud provider service levels
🟨 Consumer responsibility
🟦 Provider responsibility

Figure 1: Control Level of Cloud Computing.

All of these features and facilities maximize security risks on the Cloud, open many doors for hijacking, and increase possible system vulnerabilities. Risks will be eliminated or mitigated by a robust governance framework (Furht and Escalante, 2010, pp. 3-21) (Buyya and Broberg et al., 2011, pp. 573-593).

Governance consists of policies, guidance, processes and decision-rights for a given area of responsibility. Corporate governance is to align processes and policies with business to ensure arrival to the business objectives. IT governance is part of the corporate governance and focuses on IT decisions and policies to ensure that IT assets are used according to the approved policies and procedures (workshop 116, Security, Openness and Privacy – Cloud Governance, 2011).

IT assets are huge and distributed between customer and service provider premises. They are classified into many types like people, policies, and equipment. It may be inside the organization or outsourced. Here, governance is required to control and maintain assets.

In many organization success stories, there is a harmony between managing the IT assets and decisions made by management. DELL Supply chain success story is an example of this harmony (Mcwiliams and White, 1999).

IT governance is responsible for aligning the IT assets with the business goals and strategy to deliver values to the entity. Cloud Computing Governance is part of the IT governance in the organization's governance hierarchy.

Governance is to control and secure our data outside our organization premises. It will align business speed to the Cloud and will cope with market demands. It helps also to initiate a new IT operating model (Mather and Kumaraswamy et al., 2009, pp. 176-202).

Organizations must ensure that the level of access they request is guaranteed into the Service-Level Agreement (SLA); uptime must be audited regularly to ensure that it conforms to the SLA (*IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud,* 2011). There are many ways to mitigate risks in the Cloud using technologies and policies (*Guidelines on Security and Privacy in Public Cloud Computing,* 2011). Cloud governance makes the decision easier and balances the investments and risks while gaining the Cloud benefits (Enisa.europa.eu, 2014) (Morin and Aubert et al., 2012, pp. 5509-5514).

Processes, policies, tools and even organization personnel will be unified under one framework that makes the workflow easier and give the business some elasticity on applying the framework.

A Cloud governance should contain processes to apply Cloud Computing inside the organizations and applied controls to facilitate it. Moreover, it must adopt the organizational roles and responsibilities to ensure better support of implementing Cloud Computing governance. Finally, it should use all available technology tools that will help to apply the governance framework.

When implementing security governance, we need well-articulated policies and procedures including controls. Security controls is the key to apply security governance. CSA CCM is a well-defined industrial security control list (Cloudsecurityalliance.org, 2014). We will distribute these controls on the theoretical Guo's model for aligning the model with the Cloud market. We will demonstrate CSA CCM and Guo's model in the next two subsections (Guo and Song et al., 2010, pp. 1-6).

2.1 Cloud Control Matrix

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is an initiative from CSA to determine the baseline of security. It leads the Cloud market and helps customers assessing the risks of all Cloud domains.

The CSA CCM provides a controls framework that covers almost all Cloud security domains. CSA relates it to the standards already in the market for IT Governance like COBIT. They mapped controls to the industry and practical life that help during the process of transferring the Guo's Model from theoretical model to practical model.

As a framework, the CSA CCM offers to the organization the required structure and details related to information security tailored to the Cloud industry. It covers all Cloud aspects and controls. Some controls are covered in IT governance models and other controls, related to the Cloud system, are brand new.

By mapping these controls to security standards that are already implemented in the market like COBIT and HIPPA, it helps in pointing to information security control required by business and management strategy (Sahibudin and Sharifi et al., 2008, pp. 749-753).

The main target of CSA CCM is to provide a standard management to security and operational risk that will face any organization implementing Cloud Computing in its infrastructure. This matrix is mitigating and minimizing security threats and vulnerabilities in the Cloud by providing controls to each domain that covers almost all Cloud security related topics.

CSA CCM contains eleven domains that cover all security issues related to Cloud computing. They divide it by function. It means that controls related to legal issues will be a domain and controls related to data governance will be a domain and so on.

Compliance is the first domain. It has six controls that cover audits, regulations, and intellectual property. It also reviews legislative, regulatory and contractual requirement. Data governance has eight controls that manage data objects containing information. It classifies and assigns responsibilities, communication, labelling, policies, and data destruction. Facility security has eight controls that secure working environment like physical access, site authorization and asset management. Human resource security has three controls that cover aspects related to humans like background screening and employment termination.

Information security is the largest domain in CSA CCM; it has thirty-four controls that take care of security management, policy, user access, training, benchmarking, encryption, security incidents, infrastructure and auditing. Legal is the domain that controls agreements and reviews contracts with the national and international laws. It has only two controls. Operation management is taking care of resources planning and managing procedures and equipment. Risk management is a very important part of the matrix. It predicts all risks happening in the Cloud or the project. It delivers a plan to control and mitigate risks. Release management controls planned changes in production environment and set policies and procedures to apply the new changes. It has five controls.

Resiliency is responsible for business continuity planning and environmental risks mitigation. It has eight controls. Security architecture is the last domain containing fifteen controls that address all regulatory requirements for customer access, data security, network security including infrastructure and applications.

2.2 Guo's Governance Model

The Guo's Governance Model can be identified as the first proposed academic governance model to our knowledge (Figure 2). It outlines the necessary components for Cloud governance. It was created based on four objectives of Cloud governance, which are service, policy, risk, and compliance management. It classifies the components of Cloud governance into three categories; policy, operational and management activities.

There is a gap between the model and the real world, which we cover in this paper. We contribute in this paper to close this gap. The gap in the model can be identified after we apply controls in the CCM to the Guo's model. The CCM is a list of controls extracted from real Cloud business. We can apply it to any Cloud Computing system and be sure that most security aspects are covered. It helps transferring the theoretical model to an applicable one.

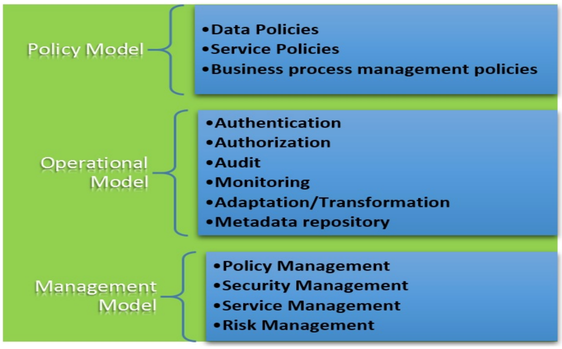


Figure 2: Guo's Governance Model.

First missing corner in the model is the aligning with business strategy. The gap between IT and organizational alignment obstructs the adoption of Cloud computing. In Cloud Computing system, an organization's IT team has to be upgraded from being only technologists towards being also information and business experts. Therefore, the organization should determine how Cloud Computing could best serve its business needs while addressing how it may affect its current IT organization and governance.

In the Cloud, the traditional roles of CIO, IT support, service provider and even user are changing dramatically. Organization applying security roles should align it with the whole organization's roles. It has to assure the harmony between controls and roles governing the organization. This integration makes implementation easier and changes the way employees can accept and apply these roles and responsibilities. This is the second missing corner.

Roles and responsibilities may change during or after implementation of the Cloud system. Therefore, change management should have a well-defined strategy because of the nature of Cloud. It changes periodically and rapidly more than any other fixed systems. Replacing defective items, applying patches, or upgrading firmware are a few examples of the change procedures needed in Cloud environments. Taking resources down for change, applying efficient change management techniques is a key to survive in the Cloud. Change management is the third missing corner in the model.

Feedback process in a successful system improves the efficiency and reliability. Using Cloud feedback process gives all parties the ability to ensure that the system performs as expected. Guo's model does not clearly state this type of feedback. Service feedback is the fourth missing point in the model.

Due to asset distribution in the Cloud environment, asset management will be an important part of Cloud governance. It should be stated clearly. Assets management changes depending on the type of implementation and the agreements between the parties. Asset management is another missing point in the model.

Last missing point is the exit strategy. It contains contract ending, data and systems maintenance and it manages assets before and after exit. A Cloud exit strategy should be as simple as putting data in the Cloud, but this is far from the case, especially in case of proprietary public Clouds.

3 OUR PROPOSED DEFINITION OF CLOUD GOVERNANCE

Cloud governance definition is still in the developing mode. Cloud Computing Use Discussion Group (2010) defines Cloud governance as "the controls and processes that make sure policies are enforced" (Cloudusecases.org, 2010). Many organizations and groups define the Cloud Computing governance in a different ways.

According to our definitions, defining policies is important, but defining processes to apply these policies is more important. Cloud governance model should be aligned with corporate governance and IT governance. Moreover, it has to comply with organization strategy to accomplish business goals.

In our experience, Cloud governance has to support business strategy and to ensure service value, service quality and security irrespective of the control and locations of the services. Therefore, we define Cloud governance as:

"Cloud governance is a framework applied to all related parties and business processes in a secure way, to guarantee that the organization's Cloud supports the goals of organization strategies and objectives."

4 NEW MODEL PRESPECTIVE

Cloud governance is challenging. Technology is faster than the standards. We have to take into consideration the future expansion and update.

Building Cloud governance increase the ability to its technology to grow not to hinder it (workshop 116, Security, Openness and Privacy – Cloud Governance, 2011). The governance process guarantees the rights of all stakeholders.

The challenge is the trade-off to achieve a governance model's implementation plan agreed by all parties. The plan should be elastic and customizable to all models and business cases. The plan has to tolerate moving between the Service Providers (SP) and their customers.

The vague nature of information interchange, the ubiquitous connectivity and the old static controls, all require new thinking with regard to Cloud computing. How can we implement the governance model without knowing the practical controls from real world and its implementation?

Therefore, what we already did is transforming the Guo's model to an applicable framework. We distribute controls under each model and its components to illustrate the practical implementation of the governance. We categorize the controls into two main categories, normal controls and key controls. We reserve developing the criteria to measure each control for future publications.

As we have seen, the Guo's model is not a process oriented. To overcome the problem, we redefine its three models (policy, operational, and management) to be processes. Then, we correlate the different CCM controls to each relevant process. Thereafter, we create new processes for the controls that are not relevant to any existing process.

We have to go deeply inside each model to determine the related controls to achieve the goal of this model. The model should be understandable and the structure of the model should be logical and reasonable.

To solve these issues we add, modify and update few categories of the Guo's model (Table 1). In the Management Model, we define clearly the Roles and Responsibilities under the Security Management. We use it in aligning Cloud system roles with the organization's roles and responsibilities. In addition, we have added Service improvement to the Service Management to be used as a key of the feedback to increase system reliability and efficiency.

Table 1: New Cloud Governance model.

New Governance Model		
Policy Model	Operational Model	Management Model
Data Policy	Authentication	**Policy Management**
Service Policy	Authorization	• Generic Policy Ontology
Business Process Management Policy	Audit	• Application Specification Ontology
Exit Policy	Monitoring	• Policy Repository
	Adaptation/ Transformation	• Policy Specification Service
	Metadata repository	**Security Management**
	Asset Management	• Integration
	• Human resources	• Privacy
	• IT Assets	• Access
	Configuration management and documentation	• Jurisdiction
	Capacity planning	• Roles and responsibilities
		Service Management
		• Service Discovery
		• Service Delivery
		• SLAs management
• Note Grey cell is the identified gap. Bullet is a sub items		• Errors and exceptions management
		• Auditing and Logging
		• Service improvement
		Risk Management
		Change management

Change Management will be part of the Management Model due to the rapid changes in the

Cloud service either from the customer side or from the provider side.

Under the Operational Model, we define the asset management, configuration management and capacity planning. It supports the organization to operate its own Cloud or the Cloud services they use. Moreover, we have added Capacity planning to enforce changing the way of thinking inside the organization regarding the Cloud service. It helps in the planning phase and it guides the organizations to meet future changing demands of its services. Moreover, it supports the organization to take the right decision about Cloud service.

Finally, we have added the exit policy to be stated clearly and be defined in any contract separately to well define the procedures to be done to maintain user systems and data after ending the Cloud service or moving to a new provider. It supports both sides to be secure before or after service contracting.

Now we have processes in the new model and each process has its own controls. Each control has inputs and outputs. Control's measures and tools depend on the deployment model. We create a framework and put each process in its suitable stage. The new framework is a conceptual structure to serve and guide organizations in Cloud Computing adoption process.

5 NEW CLOUD GOVERNANCE FRAMEWORK

The changes being driven by Cloud Computing and the growing sophistication of attackers do represent new challenges. We solve these challenges by creating the Cloud Governance Framework to control people, data, applications and infrastructure. Our security framework provides a more integrated, intelligent approach to Cloud Governance.

An intelligent framework must improve itself continuously; it has to have a feedback and service improvement process. We develop a new framework with five stages to achieve this goal (Figure 3).

It also solves the weakness of organization strategy alignment. The stages are:

- Strategic trigger
- Define and align
- Build and implement
- Deliver and measure
- Operate and feedback

Strategic trigger is the first stage. It is the event that initiates the need to use the Cloud computing.

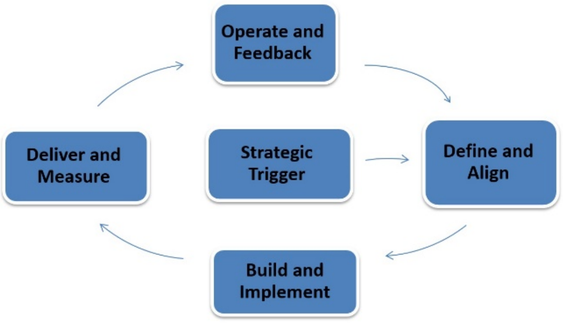


Figure 3: New Cloud Governance Framework.

Business need is the main trigger for using the Cloud services. Other trigger may be gaining market share due to strong competition in market. The company needs a competitive edge. We use Cloud services to comply with a standard or a government rule. The major trigger is the technical need. An SP delivering services needs technically a Cloud service (Heier and Borgman et al., 2012, pp. 4982-4991); for example, E-mail services.

This stage contains four processes. Business process management policy defines interrelations between Cloud-based services. It analyses the business and considers the service process reuse. Service discovery finds and discovers the existing services and available technologies for new services. Capacity planning reviews the existing environment and future business extensions to plan the best way technically and financially to achieve business goals. Exit policy is mandatory. Business needs changes to cope with the market. It may require ending the Cloud service. Exit the Cloud service is more complicated than joining and entering it. A well-defined plan is mandatory before starting to use Cloud service.

Define and align stage is the planning phase of adopting the Cloud service or transforming the existing environment to the Cloud. It ensures that the Cloud services are aligned to the business needs and actively supports them. Organizations using a Cloud require their service to be successful. If processes and services are implemented, managed and supported in the right way, the business will be more successful. This means cost reduction, revenue increase, and achieving its business objectives. It is the most important phase helping the decision makers with the economic and technical preparations for Cloud services.

This stage contains six Processes. Data Policy defines data's physical and logical model, in addition to data performance and stability. Service policy builds a service dictionary. It analyses the integration and separation of the service based on deployment model. Policy management determines and reviews the service policy. Moreover, it reviews the violation and solves the policy conflicts in order to prevent further problems. Risk management defines risks when moving to the Cloud. It plans a mitigation process and determines residual risks. Risk plan has to be reviewed with the organization and provider policies. Jurisdiction is an important process. Law and regulations vary from country to another. Organizations must review country laws where data is to be stored and processed. Integration is a mandatory process if you have an existing infrastructure. It plans the integration between the existing environment and the Cloud service.

Build and implement stage covers issues related to people, processes and infrastructure technology. It ensures cost-effective and the high quality provision of Cloud service necessary to meet business needs. The blurred lines between the traditional technology and Cloud services management means that an updated approach to managing Cloud implementation is needed. This stage contains eight processes. Authentication determines the authentication mechanism that will be used in the Cloud and between organization systems and Cloud. Authorization is the level of access that will be granted to users from the organization side and from the provider side as well. Metadata repository is the storage of policy. It considers the location of polices and roles. Asset management monitors and maintains things of value to an organization. It manages the logical and physical assets and even human assets. Configuration management and documentation establishes and maintains performance, functional and physical attributes. It also establishes and maintains configurations within Cloud service throughout its life. Roles and responsibility is a dictionary, which determines the roles and the responsibility of each contributor in the Cloud service. Privacy considers the data encryption and the location privacy. Access takes care of the access policy in the Cloud because of using shared resources.

Deliver and measure stage ensures that the implemented service is aligned with the planned services. It measures and compares the outputs with the references that were determined before. This stage contains four processes. Service delivery is moving the service to the execution environment. SLA Management ensures that all service levels are met. It reviews contract for penalties. Errors and expectation management reviews the current environment with the planned one. It analyses the running systems and reports the existing errors. Auditing and logging track all the activities and define whom, when and where this activity was done. It helps during external and internal auditing.

Operate and feedback stage is the final stage in the framework. Feedback for many organizations becomes a temporary project recalled only in case of malfunction or failure that affects the business. After resolving the issue, the concept is forgotten until the next failure occurs. The most important task starts after implementation. How do we gain benefits of using the new service? How do we measure, report and operate the new service to improve the service delivery? This requires wise decisions to operate and control feedback. It clearly defines goals, documented procedures, and identified roles and responsibilities.

This stage contains four processes. Monitoring collects transaction and access data to present a service statistics. It helps the management to review the existing environment and to plan for the future expansion. Adaptation/transformation manages the unavoidable consequences and changes in the running service. Service improvement assesses measures and improves everything in the system. It uses all the data collected in the execution phase. Change management transforms the service to a desired future state. Due to rapid changes in technology, the organization must cope with these changes. All changes have to be approved from all parties.

We can apply this framework to any Cloud system. We need controls and tools that can activate each process inside the framework. We have to state controls under each model and its components. We classify the controls into two types, key control and normal control. Key control is the control that will be mandatory and necessary to apply this process into the framework. Normal control is the control that has some inputs but is not mandatory to achieve the main goals of the process. We have distributed ninety-eight controls from CSA-CCM on each process in the framework. Then, we determine the key and normal control. Due to limited space, we will publish the details at many future publications.

6 CONCLUSION AND FUTURE WORK

A Cloud system has different deployment models and architecture. Although it offers an economy of scale solution to the market, it creates new risks and challenges in the IT environment. In this paper, we introduce our new Cloud Computing governance model that represents a perspective combination of theoretical and practical implementation. We turn the Guo's theoretical model to a practical model to enable applying it to the industry. We identify the gap using CCM, and then identify controls related to each process and its effect using CCM. We add, modify and update the missing corners in the model. We create a new governance framework. It is a five stages framework with a service feedback. Each stage has few processes. Each process contains controls. Each control has inputs, outputs, and tools to activate and measure it. The framework is suitable for all Cloud deployment models. In the future, we will apply the new governance model and framework to all Cloud models (SaaS, PaaS, and IaaS). We will specify inputs and outputs to each control. We will define the RACI (Responsible, Accountable, Consulted, and Informed) Model and identify persons that must be informed and accountable based on the deployment model. In addition, we will extract and develop SLA from the new Cloud governance model. We will relate controls effect directly the SLA.

REFERENCES

Ahmad, R. and Janczewski, L. 2011. Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective. pp. 372-379.

Borgman, H. P., Bahli, B., Heier, H. and Schewski, F. 2013. Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. pp. 4425-4435.

Buyya, R., Broberg, J. and Goscinski, A. 2011. *Cloud computing*. Hoboken, N.J.: Wiley.

Cloudsecurityalliance.org. 2011. *Cloud Controls Matrix (CCM): Cloud Security Alliance*. [online] Available at: https://Cloudsecurityalliance.org/research/ccm/.

Cloudusecases.org. 2010. *Cloud Computing Use Cases group*. [online] Available at: http://Cloudusecases.org.

Copie, A., Fortis, T., Munteanu, V. I. and Negru, V. 2013. From Cloud Governance to IoT Governance. pp. 1229-1234.

Enisa.europa.eu. 2014. *Cloud Computing Risk Assessment — ENISA*. [online] Available at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/Cloud-computing-risk-assessment.

Foster, I., Zhao, Y., Raicu, I. and Lu, S. 2008. Cloud Computing and grid computing 360-degree compared. pp. 1-10.

Furht, B. and Escalante, A. 2010. *Handbook of Cloud computing*. New York: Springer.

Guidelines on Security and Privacy in Public Cloud Computing. 2011. [e-book] USA: NIST. Available through: http://csrc.nist.gov/publications/PubsSPs.html http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Guo, Z., Song, M. and Song, J. 2010. A governance model for Cloud computing. pp. 1-6.

Heier, H., Borgman, H. P. and Bahli, B. 2012. Cloudrise: Opportunities and Challenges for IT Governance at the Dawn of Cloud Computing. pp. 4982-4991.

IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. 2011. [e-book] ISACA. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx.

Li, J. Z., Chinneck, J., Woodside, M. and Litoiu, M. 2009. Deployment of services in a Cloud subject to memory and license constraints. pp. 33-40.

Li, X., Zhou, L., Shi, Y. and Guo, Y. 2010. A trusted computing environment model in Cloud architecture. 6 pp. 2843-2848.

Mather, T., Kumaraswamy, S. and Latif, S. 2009. *Cloud security and privacy*. Beijing: O'Reilly.

Mcwiliams, G. and White, J. 1999. Dell to derail: Get into gear online. *Wall Street Journal*.

Mell, P. and Grance, T. 2011. *The NIST definition of Cloud computing*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Morin, J., Aubert, J. and Gateau, B. 2012. Towards Cloud Computing SLA risk management: issues and challenges. pp. 5509-5514.

Mukherjee, K. and Sahoo, G. 2010. Cloud Computing: Future Framework for e-Governance. *International Journal of Computer Applications*, 7 (7), pp. 31-34.

NIST Cloud Computing Security Reference Architecture. 2012. [e-book] USA: NIST. Available through: http://csrc.nist.gov/publications/PubsSPs.html, http://collaborate.nist.gov/twiki-Cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf.

Popovic, K. and Hocenski, Z. 2010. Cloud Computing security issues and challenges. pp. 344-349.

Sahibudin, S., Sharifi, M. and Ayat, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. pp. 749-753.

Workshop 116, Security, Openness and Privacy – Cloud Governance. 2011. *Internet Governance Forum*. [online] Available at: http://igf.wgig.org/cms/component/chronocontact/?chronoformname=WSProposals2011View&wspid=116.