Cloud Computing: Governance, Risk Management and Audit of IT Services

D Venkatesh
Department of IT, CBIT, Hyderabad,Telangana,INDIA

Vijay Kumar Damera
Department of IT, MGIT, Hyderabad,Telangana,INDIA

Suresh Pabboju
Department of IT, CBIT, Hyderabad,Telangana,INDIA

Abstract – The services of the "Cloud", commonly known as Cloud Computing, are increasingly present in the context of service providers to operate in the market of it. The move to the "Cloud" is often related to a vision of lower costs and greater business opportunities, generated by a new IT service delivery model. However, there are risks and threats that need to be mitigated by contributing to effective governance of these services, the definition of performance metrics and the implementation of permanent monitoring mechanisms.
In this context, the Cloud Computing model has features that distinguish it from traditional cloud computing models. The risks are different for each IT service model in the Cloud and are different for each implementation model. To that extent, it is vital to clarify the concept underlying the model and critical areas of operation, such as the way to more accurately identify existing risks and thus assess the degree of threat they pose to companies.

Index Terms – Cloud Computing, IT Governance, Risk, Audit of IT Security, Cloud Services Provider, SLA, SaaS, IaaS and PaaS.

1. INTRODUCTION

In recent years, Information Technology (IT) services in Cloud infrastructure, platforms and applications have grown exponentially in response to market challenges, subject to extreme variations that require rapid and flexible IT responses, but also because of economic constraints that have long ceased to be cyclical.

Capgemini's latest "Quality Report 2013-2014" [ISACA Journal - BIG DATA, 2014] estimates that 32 percent of all software testing refers to applications in the Cloud while another Gartner study "Gartner Identifies Seven Major Projects CIOs Should Consider During the Next Three Years " estimates that the Cloud Computing market will reach $ 350 billion USD by 2018 so this trend should not be overlooked, nor by IT service providers in Cloud, Cloud Services Providers CSP) nor by the client companies that can benefit and leverage your business from these services.

The main reasons why companies opt for cloud computing are generally associated with the characteristics of the service, which emphasizes greater efficiency in the management of IT resources, greater agility and access to innovative technologies and, therefore, greater competitiveness in the the market in which they operate and the lower costs of IT investments.

The impacts on the management and daily operations of companies are, however, numerous:

Security risks, threats of disclosure of the privacy of sensitive business data, risks of availability of services or risks of compliance with legal and statutory requirements [Thor Olavsrud, 2012].

The news gives us, almost daily, examples such as the ones we have just mentioned. For example the large-scale failure of Amazon's services in 2011, DropBox vulnerabilities that allowed users to access other users' data without authorization or even the recent cases discussed at the National Security Agency (NSA) level of Edward Snowden [ISACA Journal - BIG DATA, 2014]

In the end, there are some risks that are difficult to overcome for companies, Cloud Services Customer (CSC), consider migrating their enterprise IT services to a Cloud Computing model [COBIT5 Security, 2012].

These aspects reinforce the argument of the need of these risks should be treated and controlled so as not to interfere in the strategic alignment of Cloud Computing with the objectives of the client's business.

In this paper we will reflect on this set of aspects that should be considered prior to the change of IT services to the Cloud. Let's begin by:

- Defining with greater precision the concept Cloud Computing according to the definition of the National Institute of Standards and Technology (NIST) and the current paradigm BPaaS and ITaaS 3, defined later, and the main aspects that characterize and distinguish the traditional computing models in the "cloud".

- Then we will identify the main risks and threats that weigh upon the decisions inherent to the passage of IT services to the Cloud.
- Finally we identified the role of the IT Governance and the role played by the audit of Information Systems (ASI) in the identification and mitigation of risks of this business model of IT services in the Cloud.

2. CLOUD COMPUTING

According to the definition of the National Institute of Standard and Technology [NIST 2012], Cloud Computing is a model that allows access to the customer's request, a set of shared resources of Information Technologies (IT), for example, network components, servers, storage and computer applications, quickly provided and available, with a minimum of effort and interaction on the part of the cloud service provider (CSP) [HARDING 2011]. You qualify this way due to their five essential characteristics, their three models of service and four deployment models, illustrated in figure 1.

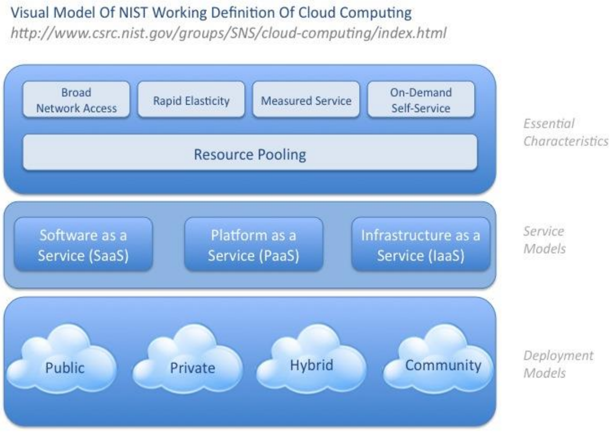
Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

Figure 1 - NIST visual model of Cloud Computing Definition [CSA 2012]

The concept of "as a service" can still be applied to business processes, although it is not included in the taxonomy of the Cloud Computing 2.0 model, such as payroll, CRM and billing, by Business Process as a Service (BPaaS) [IBM DeveloperWorks, 2012]. BPaaS differs from SaaS by including cloud services partly run by people and not just by software applications [Mike Kavis, 2013].

At another level we still enable *IT as a Service* (ITaaS), since that provided by *Cloud Services Providers* (CSP) which includes the amount of IT services, including *hardware*, software and support, so that the *Cloud Services Customer (CSC)* can manage your business and its information systems as a whole (SaaS, PaaS and IaaS) [VMWARE CIO, 2012].

These aspects, fundamentally those that are part of the NIST taxonomy, as a whole and at the same time distinguish Cloud Computing from other traditional models of computing in the "Cloud".

There are numerous economic and operational advantages for organizations, but there are also many challenges and obstacles that companies, CSCs need to analyze. Advantages that arise from the availability, speed, flexibility and scalability in the provision of IT services, which are made available to the customer's request and according to their needs. On the other hand, the motivation for a smaller CAPEX4, since it adopts a pay-as-you-go concept, without initial investment in hardware or software, at the same time that the company is freed of the weight and the burden of the management technology. But the migration of a part or all IT infrastructures to a CSP does not relieve the client company, the CSC, to third parties, stakeholders and shareholders of the possible negative results and impacts that may result! When choosing services in the Cloud, it is vital that the company has the know-how, skills and internal capabilities that ensure proper monitoring of the quality of services provided by Cloud Services Providers (CSP). This issue is perhaps one of the first challenges of IT security professionals who have to deal with a new paradigm of services, a paradigm that is largely related to the level of abstraction that incorporates the Cloud Computing model, as we will explain further [ISACA Journal - BIG DATA, 2014].

The following challenges result from the loss of direct control and sense of physical location of the data, the potential risks associated with resource sharing, namely application, due to the multitenancy5 characteristics of the model, but also, not least, to dependence and loss of autonomy for third parties, of IT services [CLOUD COMPUTING 2012].

3. RISKS OF CLOUD COMPUTING

Security and privacy are, as we have seen, the most frequently mentioned concerns and also the biggest obstacles to the adoption of IT services in the Cloud. Nevertheless, Cloud Computing risk analysis differs not only in each of the service models, but also in each of the implementation models that are adopted.

For the various service models, one of the immediate implications of the decision to move to Cloud is that information assets are managed by Cloud Services Providers (CSP), making it transparent and abstract to the customer, CSC, the technology and the processes that support those assets. This lack of visibility, also called the abstraction layer, is the common denominator in all service models and extremely important for an adequate risk assessment [COBIT5 Assurance, 2014].

Each model corresponds to a certain level of abstraction, as we can see in Figure 2, which increases as the number of service layers provided by the CSP increases.

The Infrastructure as a Service (IaaS) model corresponds to the lowest level of abstraction, since it only includes infrastructure such as installations, hardware, storage and processing resources, while the Software as a Service (SaaS) model corresponds to the highest level of since it includes applications, platforms (middlware) and all infrastructure. In this last model the CSC client ignores the layers that support the application software and this means that the higher the level of abstraction, the greater the risk and therefore the greater the threats that must be taken into account. It is this cumulative aspect of risk that exists in the Cloud service models [CLOUD COMPUTING 2012], which should be considered in the risk analysis of this model.

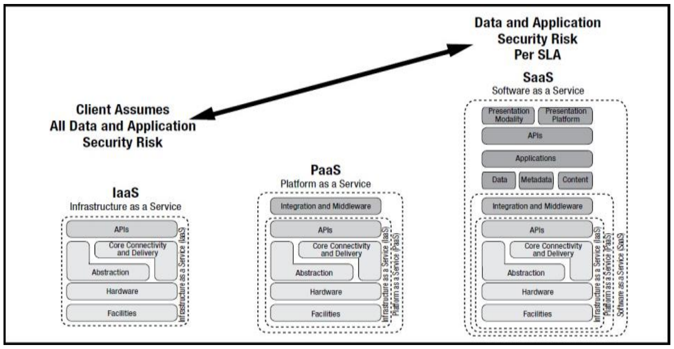

Figure 2 - Service Models of Cloud Computing CLOUD COMPUTING source: [2012]

According to ISACA, "Security Considerations for Cloud Computing" [CLOUD COMPUTING 2012] identifies and characterizes the potential risks of events with a negative impact, classified according to the threat they pose to the client company , the Cloud Services Customer (CSC). These risks are typified in Information Unavailability, Loss, Theft, or Disclosure of Sensitive Data and are listed below, in accordance with each service model (IaaS, PaaS, SaaS) and then for each of the Public Implementation Models , Private, Hybrid and Community.

A) Risk Factors of Infrastructure as a Service (IaaS) Model

The IaaS service model allows a CSC to use a certain infrastructure, which can go from the premises to accommodate computer equipment in a perfectly controlled environment, to the equipment itself, such as servers, processors, RAM, storage space and services (switching and networking). Among the several risks inherent to this service model we highlight the following, according to ISACA in "Security Considerations for Cloud Computing" [CLOUD COMPUTING, 2012]:

1. Cross-Border Legal Requirements - assumes the risk of disclosure - when the Cloud Service Provider (CSP) operates outside the territory, in countries with different legislation, it is necessary to identify all legal requirements to ensure that the Cloud Services Consumer (CSC) is not to violate the laws of that country to store and process your data through the CSP infrastructure.
2. Multitenancy and Insulation Failure - incorporates risks of theft and/or disclosure - one of the great benefits of Cloud lies in the possibility of sharing hardware and software resources by various entities (tenants). In the multitenant environment it is essential that the shared resources are completely isolated and protected so that there is no disclosure of data by other tenants, for example in situations of reallocation of resources, this being the risk that must be controlled and mitigated.
3. Lack of Visibility of the Technical Measures of Security on Site - includes risks of loss, theft, unavailability and/or disclosure - it is the responsibility of the CSP provide the contracted capacities, ensuring that there is no security breaches through a Appropriate governance and security policy that meets the customer's needs.
4. No Disaster Recovery Plan (DRP) and Backup - includes the risk of downtime and/or Loss - this factor implies a high degree of risk by the CSP shall ensure these basic preventative measures aligned with the needs of the CSC.
5. Physical Security - Integrates Risk of Theft and/or Disclosure - in IaaS model in which resources are shared by several entities, it is essential that the CSP ensure physical security measures [ISO/IEC 27002:2013] that prevent unauthorized access or destruction of sensitive information or vital.
6. Elimination of Data - Includes Risk of Disclosure - the CSP shall ensure appropriate measures of destruction of information after ending the contracts, in order to avoid the retrieval and dissemination of information is critical and sensitive of the CSC.
7. Offshoring Infrastructure - integrates risk of unavailability, Loss, theft and/or disclosure - the shift to an infrastructure offshoring increases the likelihood of attacks that can affect the organization's assets in the cloud. Usually these attacks are perpetrated through communicatestions, exposing both the "cloud" as the internal infrastructure of organizations, both of the CSC as the CSP.
8. Maintaining the Security of Virtual Machines (VMs) - Risks of unavailability, Loss, theft and/or disclosure - one of the features of IaaS is to allow the customer to createvirtual machines (VMs) in several states (active, suspended or stopped) and in spite of the CSP to be involved in the process of maintaining these machines in general is the responsibility of the customer, i.e., the CSC. This could jeopardise the security of the entire

infrastructure when they are linked VMs that have been disconnected for long periods, without the respective security updates.

9. Authenticity of Cloud Servive Provider - incorporates risk of unavailability, Loss, theft and/or disclosure - it is the customer's responsibility of IT services in the Cloud the verification of the authenticity and credibility of the CSP, in particular as regards its "Health" Financial, profitability of the past 3 years, market references and guarantees to third parties.

B) Risk factors of Platform as a Service (PaaS) Model

The PaaS service model adds an abstraction layer to the previous service model, IaaS, where the physical infrastructure, operating systems, and development tools are the responsibility of the vendor, the CSP, and the applications and data processed are responsibility of the company, the CSC. According to ISACA [CLOUD COMPUTING, 2012], this service model has the same risks as the IaaS model, plus those indicated below:

1. Installed Capacity - Includes risks of theft and/or disclosure - the risk increases to the CSC when the features provided are disproportionate to the resources and capabilities of the CSP. This situation can introduce vulnerabilities and cause abnormal behavior or a lack of performance that impact the organization.
2. Vulnerabilities of Service Oriented Architecture (SOA) - Includes risks of unavailability, Loss, theft and/or disclosure - the use of libraries sounds, the responsibility of the CSP, reduces the time of development and testing in the Cloud, but may introduce vulnerabilities on platforms, not always visible to the customer.
3. Disabling the Applications - Incorporates risk of unavailability, Loss, theft and/or disclosure - backups and copies of security, as well as the originals of the applications developed in a PaaS environment, must always be available and updated in Possession of the CSC, in the event of a termination of the contract or amendment of their respective terms in which the services are to be provided.

C) Risk factors of Software as a Service (SaaS) Model

In this service model CSP provides the ability of the CSC company to use computer applications in the cloud infrastructure. All the infrastructure, namely hardware, operating systems and applications are from CSP and CSC is only responsible for data processing, with end user functionalities. According to ISACA [CLOUD COMPUTING, 2012], this model has the same risks as the previous service model, PaaS, plus those indicated below.

1. Elimination of Data - includes risks of theft and/or disclosure - In the event of termination of the contract, the data entered in the application of CSP should be immediately removed, using forensic tools to avoid disclosure and the breach of confidentiality.
2. Lack of visibility on the SDLC - integrates risk of unavailability, Loss, theft and/or disclosure - companies that use applications in the Cloud does not always have visibility on the development life cycle (SDLC) systems. Do not know in detail how the applications have been developed and are unsure why the security measures implemented. This can lead to a discrepancy between the security offered by the application and the requirements demanded by the CSC.
3. Identification and Management of Access - incorporates risks of loss, theft and/or disclosure - to maximize revenues, the CSP provides service and applications to multiple customers on the basis of sharing of servers, applications and data. Nevertheless, if there is an adequate management of access, a client can have access to the data from another client without the proper control and even without the knowledge of the CSC.
4. Exit Strategy and Portability - includes risks of unavailability, Loss, theft and/or disclosure - one of the major constraints that presents itself to companies in time to terminate a contract with a CSP is the question of how to migrate the data to another CSP or even for services in house without any loss of data or with a minimum of effort for reconstruction of those concerned. May not exist tools that ensure the portability of data or even the absence of compatible applications that give continuity to its processing which may cause disruption of services with losses and impacts that must be anticipated and mitigated by the CSC.
5. Greater exposure of applications to attacks - integrates risk of unavailability, Loss, theft and/or disclosure - a computing environment in "cloud", the applications, which often interact with applications in the cloud, have a greater exposure to attacks. Not all network firewalls standards are sufficient, which implies the need for additional security measures that restrict the range of possible attacks.
6. Lack of control over the applications - includes the risk of downtime and/or loss - the CSP has sometimes need to introduce corrections in their applications quickly, without waiting for formal approval of their clients. In these cases, the CSC may not have control over the processes and be hindered by unforeseen effects.
7. Vulnerabilities in browser - incorporates risk of unavailability, Loss, theft and/or disclosure - In most cases the SaaS services are made available through web browsers which, unfortunately, are tempting target

for malware or other attacks to CYBERNAUTS. If the customer's browser is infected the access to data and applications can be compromised.

D) Risk factors of Public Cloud Deployment Model

The type of implementation does not have the same abstraction as the service models, since in this case the risk is not cumulative but rather particular to each model. In a public implementation the CSP provides an infrastructure shared by several companies and unrelated individuals. According to ISACA, "Security Considerations for Cloud Computing" [CLOUD COMPUTING 2012], the following risks are considered:

1. Total sharing of the "Cloud" - incorporates risk of unavailability, Loss, theft and/or disclosure - the infrastructure of "cloud" is shared by multiple tenants, by various CSC, without respect, common interests, or the same level of security concerns, and it is a potential risk plus for the CSC that must be analyzed and mitigated.

2. Collateral damage - includes risks of unavailability, Loss, theft and/or disclosure- in a shared infrastructure if a given customer is attacked may have an impact on other customers of the same CSP, even if they are not the objective of the target (for example DDoS attack).

E) Risk factors of Community Cloud Deployment Model

In this implementation model services are provided for the use of a group of entities that share a certain level of trust, such as a common security policy. . According to ISACA [CLOUD COMPUTING, 2012], the levels of risk are as follows:

1. Sharing of "Cloud" - includes risks of loss, theft and/or disclosure - in this model, the threat exists when different entities of the same group of companies that share the same infrastructure, have different requirements and safety measures. The procedures less demanding of one of the entities may jeopardise the SLAs of another entity.

F) Risk factors Private Cloud Deployment Model

In this model the services are provided for the exclusive use of an entity, without any interaction with other entities in the cloud. In these cases, according to ISACA [CLOUD COMPUTING, 2012], the risks are as follows:

1. Application compatibility - incorporates the risk of downtime and/or Loss - in this context it is necessary to identify and assess the degree of compatibility of legacy applications,legacy proprietary (), with virtualized environments and applications that are running in the Private Cloud;

2. Investments required - incorporates risk of unavailability, Loss, theft and/or disclosure7 - plan and justify the investment in a shared infrastructure, whether they are training and hiring required the acquisition of skills in the Cloud, it can become difficult for the CIO if the message is not properly passed to the administration of the CSC. It is, therefore, required a cost-benefit analysis, Developing a Business Case, with the strict calculation of ROI8, to determine if the "cloud" is a viable solution, whether it is aligned with the business objectives and that justifies the investment costs of the project;

3. It skills in the Cloud - includes risks of unavailability, Loss, theft and/or disclosure - even if the implementation of a "private cloud" within the organization may seem the best option, in terms of safety to its maintenance and management require special skills that can increase the costs initially specified. This analysis should be taken into account in preparing the Business Case already mentioned.

G) Risk factors of Hybrid Cloud Deployment Model

It is an implementation model that enables enterprises to mix public, private, and community cloud, depending on the level of trust requirements between enterprises. For example, a company may decide that the web portal can migrate to a public cloud but want to keep its business applications in a private cloud. This combination creates a hybrid cloud model, but the risks in this case, according to ISACA [CLOUD COMPUTING, 2012], are as follows:

1. Interdependence of Cloud - includes risks of unavailability, Loss, theft and/or disclosure - if the company CSC combines two or more different types of "clouds", you will need strict controls of identity and strong credentials to allow a Cloud has "free" and communicate with each other. The problem is, and it is difficult to manage when it has to cope with different levels of security, as has already been mentioned before.

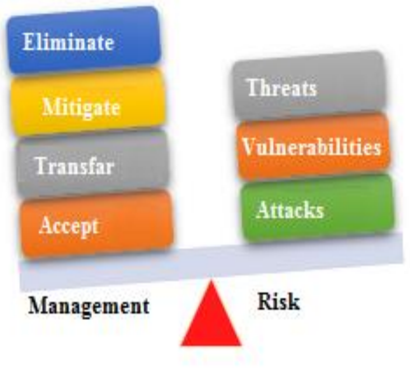

Figure 3 - Risk management measures. Adapted from: [COBIT5 Assurance, 2014]

In spite of everything that has been said so far, the risks identified for each type of service and for each model of implementation does not represent a threat level equal to all companies. They are mainly related to the activity and the size of the CSC and therefore each organization must evaluate the risk events and the impacts that may occur in your business. The actions will have to pass through the elimination, mitigation, transfer, or even acceptance of the risk, in the levels considered acceptable for the business, figure 2.

4. IT GOVERNANCE AND AUDITING OF INFORMAT ION SYSTEMS

Corporate Governance is responsible for defining principles, communicating policies, establishing rules, delegating authority to enforce these rules, and monitoring results to determine if any adjustment is required to what was initially determined.

The IT Governance, in the Portuguese translation of the original term IT Governance [ITGI - IT Governance Institute® 2008], and not "governance", which may be more appropriate for a Brazilian translation, is assumed to be a subordinate mechanism of the General Corporate Governance , with the mission of incorporating the intrinsic value of IT in all aspects of the organization.

Through IT Governance, the company takes full advantage of the information it processes, maximizes the benefits of using IT, capitalizes on opportunities and gains competitive advantage by minimizing risk and optimizing resources, Figure 4 [COBIT5 Framework 2012].

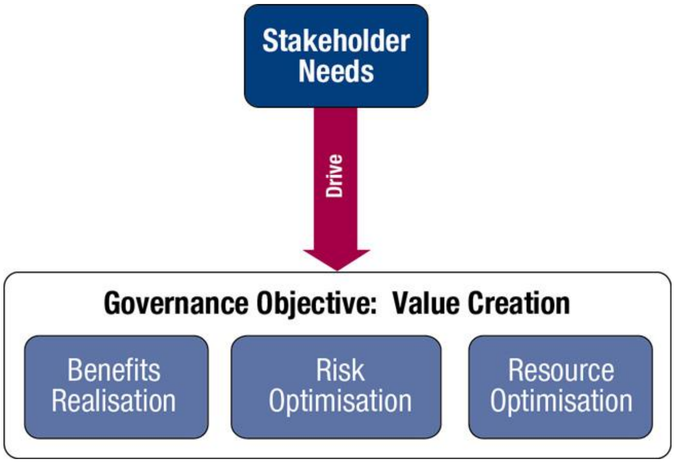

Figure 4 - Goal of governance, adapted from [COBIT5 Framework 2012]

IT Governance thus materializes good IT practices, based on proprietary IT Governance frameworks, such as COBIT 5 Control Objectives for Information and related Technology, focusing on generic processes of Evaluation, Direction and Monitoring that are broadly detailed in the COBIT framework 5 - A Business Framework for the Governance and Management of Enterprise IT. These processes aim to: maintain an effective IT Governance framework; ensure delivery of benefits; ensure the optimization of risks and resources, as shown in figure 1; and ensure a transparent policy practice for Stakeholders and Shareholders [COBIT5 Framework, 2012].

The factors that also highlight the importance of IT Governance and Cloud services follow a set of lines of concern listed below [COBIT5 Security 2012]:

1. Greater concern of stakeholders and the management of high level in relation to the widespread increase of investments in IT and return it is possible to obtain them
2. The need to optimize the costs
3. Greater compliance requirements and control of it in critical areas such as privacy and financial reporting
4. Need a careful selection of Cloud Service Providers (CSP) for greater efficiency and security of outsourcing services, acquisition and maintenance
5. Finally the need for businesses to assess their performance against the standards of reference and the area of activity of the company (benchmarking).

Information Systems audits (ASI), with its risk identification initiatives, continuous monitoring, analysis and evaluation of metrics associated with IT Governance, play a key role in the successful implementation of an organization's IT governance policies [CISA 2014].

The assurance that the risks of migration or adoption of services in the Cloud are identified and there is an adequate response to the pending threats is given by Information Systems Audit initiatives that ensure that controls exist, and are therefore implemented, which are sufficient and are being followed as expected through continuous and systematic monitoring [COBIT5 Assurance, 2014]. The objective is to provide a guarantee of comfort to internal and external stakeholders about the audited matters, ie all internal factors that contribute to the achievement of the company's objectives, called enablers by COBIT 5 [COBIT5 Assurance, 2014], all they with a given mission within the organization vital to the CSC business, as are in most cases Information Systems and Technologies.

The main objectives of Information Systems Audit are as follows [COBIT5 Assurance, 2014]:

1. Aligning itself with the mission, vision, values, goals and strategy of the organization. In short, governance alignment of IT with the company's governance
2. Achievement of performance and achievement of the

objectives set for the SI

3. Compliance with security and privacy requirements, legal, environmental and trust
4. Verification of IT investments
5. Analysis and evaluation of the risks inherent in the environment of himself as the Cloud Computing.

In sum, the Information Systems Audit process includes management at the highest level, it is transversal to all sectors and departments of the organization and focuses on two fundamental aspects, according to Figure 5 [CISA 2014]:

- In compliance, i.e., in compliance with internal and external policies and regulations and in the protection of valuable information assets for the organization
- In performance, that is, in the added value that IT represents and generates for the organization.

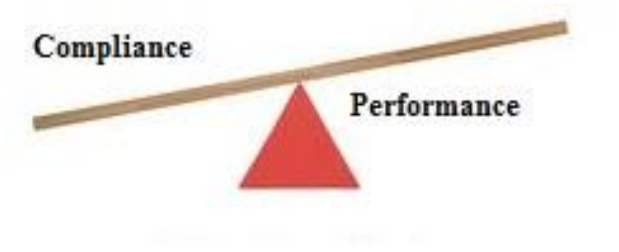

Figure 5 - Focus of Audits of Information Systems

Cloud Computing while Outsourcing should be governed, managed and audited in a way that does not compromise the business objectives. In this process, the fundamental task of analyzing and evaluating the risks inherent to the adoption of cloud-based IT services is highlighted, as a way to mitigate the occurrence of events that compromise those objectives [COBIT5 Security 2012].

The observation of several large companies, in terms of business and IT resources, shows us that one of the main reasons for the negative impacts on outsourcing IT services provided by Cloud Service Providers (CSP) often with gaps in scope clarification and definition of service levels [COBIT5 Vendor Management. 2014]. To mitigate these risks the first step is to enter into Service Level Agreement (SLA) agreements, set up controls and implement monitoring mechanisms. However, in this process, there is one key element that can never be overlooked: the trust that must prevail throughout the service life cycle, in the relationship between the CSP and the Cloud Services Customer (CSC) client company. Trust is a key element in the Cloud Computing business model. Without it, any controls and agreements will never be enough to mitigate all the risks and concerns that companies, CSC, might have about this business-IT management model [CLOUD COMPUTING 2012].

In this process, the function of the auditor is to verify the following control points [CISA 2014]:

1. Determine if the company has evaluated the advantages and disadvantages of option by Cloud Computing, in relation to their goals
2. Identify and classify the criticality of the data (private, publishes, sensitive, confidential)
3. Identify the risks referred to in the previous section;
4. Check if there is control and visibility of information critical to the business;
5. Check if they are duly contracted SLAs or whether we are dealing with Strong Service-level agreements (SSLAs) [Vaz, et al., 2013]
6. Check the best practices used by the CSP, including ISO 15504 Software Process Improvement and Capability (SPICE), CMMI and ITIL
7. Check if it is to be managed to change, which implies:
   a. Change in the processes of file, accommodation and backup of information
   b. Revision of policies of access to information
   c. Review of skills and function to manage the relationship of services with third parties (Outsourcing and Cloud)

Outsourcing governance and cloud IT service auditing thus includes the full set of responsibilities, functions, objectives and controls required to anticipate the change process, manage service introduction, maintenance, performance and CSP costs. It is an interactive process that extends to both sides, CSC and CSP, on a necessarily reliable basis, in order to ensure the continuity of IT services with adequate levels of profitability and security.

5. CONCLUSION

IT Governance, as a mechanism subordinated to the company's General Governance, assumes itself as a systematic tool of good practices to support major strategic decisions and to maximize IT investments. The effectiveness of governance is closely linked to the use of globally accepted frameworks that are independent of the size or branch of activity.

Cloud Computing should be a consequence of strategic decisions and requires continuous monitoring and control practices throughout the service life cycle, in which Information Systems Audit plays a vital role with a focus on key aspects such as compliance and performance. Trust in the relationship between the client-company and CSP, the provider of cloud computing services, is also critical throughout Cloud's service cycle. But it is in the identification and prior evaluation of the risks to the business in its specific aspects i.e., as regards the service model and the implementation model and its mitigation, that lies a great part of the success of the Cloud Computing model that we propose to validate and detail in an upcoming paper.

REFERENCES

[1] E. Weintraub, Y. Cohen, "Security Risk Assessment of Cloud Computing Services in a Networked Environment", International Journal of Advanced Computer Science and Applications (IJACSA), 7, (11), 2016.

[2] E. Weintraub and Y. Cohen, "Cost Optimization of Cloud Computing Services in a Networked Environment", (IJACSA) International Journal of Advanced Computer Science and Applications ,Vol. 6, No. 4, pp. 148-157, 2015

[3] E. Weintraub and Y. Cohen, "Optimizing User's Utility from Cloud Computing Services in a Networked Environment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 10, pp. 153-163, 2015.

[4] E. Furuncu, & I. Sogukpinar, "Scalable risk assessment method for cloud computing using game theory", (CCRAM). Computer Standards & Interfaces, 38, 2015

[5] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M Freire and P. R. M. Inácio, "Security issues in cloud environments: a survey", Int. J. Inf. Secur. 13:113–170, 2014

[6] Pappas, Vasilis, et al. "CloudFence: Data Flow Tracking as a Cloud Service. "Research in Attacks, Intrusions, and Defenses. Springer Berlin Heidelberg, 2013. 411-431.

[7] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues. " Future Generation Computer Systems 28. 3 (2012): 583-592

[8] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347-358

[9] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93-97

[10] Khalid A (2010) Cloud Computing: Applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278-281

[11] Harnik, Danny, et al. "Secure access mechanism for cloud storage. " Scalable Computing: Practice and Experience 12. 3 (2011)

[12] Song, Dawn, et al. "Cloud data protection for the masses. " IEEE Computer45. 1 (2012): 39-45.

[13] Eludiora, Safiriyu, et al. "A User Identity Management Protocol for Cloud Computing Paradigm. " International Journal of Communications, Network &System Sciences 4. 3 (2011)

[14] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, W. Lou, "Privacy-preserving public auditing for secure cloud storage", IEEE Transactions on Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[15] S. G. Worku, C. Xu, J. Zhao, X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage", Computers & Electrical Engineering, vol. 40, no. 5, pp. 1703-1713, Jul. 2014.

[16] S. More, S. Chaudhari, "Third party public auditing scheme for cloud storage", Procedia Computer Science, vol. 79, pp. 69-76, 2016.

[17] A. S Ezhil, B. Gowari, S. Ananthi, "Privacy-preserving public auditing in cloud using HMAC algorithm", *International Journal of Recent Technology and Engineering (IJRTE) ISSN*, vol. 2277, 2013.

[18] S. Jadhav, B. R. Nandwalkar, "Privacy preserving and batch auditing in secure cloud storage using AES", *Proceedings of 13th IRF International Conference*, 2014.

[19] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, W. Lou, "Privacy-preserving public auditing for secure cloud storage", *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362-375, Feb. 2013.