RESOLVING CLOUD COMPUTING SECURITY ISSUES USING ITIL SECURITY MANAGEMENT PROCESS

Attique Shah, Mazhar Ali and Aftab Ahmed

Department of Information Technology, Balochistan University of Information Technology, Engineering & Management Sciences, Quetta, Pakistan

Abstract

Cloud computing is rapidly emerging and is the most demanded segment in IT industry. It provides scalable computing resources according to the need of an organization on comparatively minor expenditure costs. Security is the biggest hurdle in the way of progress for cloud computing caused as the business data is to be released on the cloud and hence leaving a question mark on the protection of the data, due to which many business companies falter to shift to the cloud. This paper focuses on providing solutions for the security issues faced in the cloud by discussing the importance of pursuing a proper framework like Information Technology Infrastructure library (ITIL) Security Management process. There are some activities that should be performed in order to ensure the effectiveness of the security management process, which includes control, plan, implementation, evaluation and maintenance. The major benefits of this process are to adopt in a system that is continuously evolving (Cloud Computing), to support ITIL practice giving priority to security concerns and to keep in focus the Service level agreement (SLA) at the same time.

Keywords*: ITIL, SLA, OLA, SDLC, IaaS, CIA, OVF.*

Corresponding Authors' email: attique.shah@buitms.edu.pk

INTRODUCTION

Cloud computing is defined as "more than a technology". It is changing the view of how IT services are managed and consumed. As cloud computing is still emerging it has some new challenges which restricts many business companies to adopt it and many consider it as a risk to trust a third party for providing computing resources and primarily security. The biggest threat in cloud computing so far faced is security and is caused as owner lose authority over their data when they release it into the cloud. Many organizations own sensitive data and essentially require safeguarding of their data from compromising by others. These organizations hesitate to shift to cloud computing because they cannot govern their data and hence the risk of security threats can rise which causes a major drawback in implementing the cloud computing for all the organizations around the world. The best suggestion to provide a comprehensive and uniformed framework for the development and implementation of a cloud is to use Information Technology Infrastructure Library (ITIL). ITIL as a separate operational guidance called the ITIL security management and using this process we can also identify and minimize the security concerns in the cloud.

Service Level Agreement

The SLA is an officially authorized document which describes the association between the provider and the client. SLA works as a base for the agreed level of services between both of the parties. If used properly SLA should (Kandukuri *et al*., 2009).

- Identify and define the customer's need
- Provides a framework for understanding
- Simplify complex issues

- Reduce areas of conflict
- Encourage dialog in the event of disputes
- Eliminate unrealistic expectations

SLA is an iterative process and its phases are SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement (Sla Management, 2004). These four phases are very important to verify the tasks of both the provider and the client. Any misinterpretation in these phases will directly influence the system performance and security. The Qos attribute is also an important part of the SLA which changes frequently especially in an environment like cloud computing, so it needs to be examined at every phase. As cloud computing is a blend of various IT Components so it becomes very difficult to manage the QoS in it. SLA could be used as the best solution to provide QoS in cloud computing.

SLA plays a vital role in the in the overall implementation of the cloud, especially in security, as security related concerns are illustrated during the enforcement of SLA. The issues normally described in the SLA are Services to be delivered, performance, Tracking and Reporting, Problem Management, Legal Compliance, Resolution of Disputes Customer Duties, Responsibilities Security IPR and Confidential Information Termination (Kandukuri *et al*., 2009). Apart from these issues trust factor should also be considered in the enforcement of SLA.

Standardizing SLA for Security

Generally security does not get its right consideration in SLA, while it is an essential feature of the system. It is considered as an extra service and there is no such defined practice or a framework for the description of security in the SLA. Due to the irregular and altering nature of client's requirements there is a big need that the SLA should be standardized for security purpose.

One method that can be used to standardize the SLA for security purpose is to properly follow and develop it according to the Gartner seven cloud computing security risks (Brodkin, 2009). The Gartner's seven issues are basically the questions that the customer should ask from the cloud provider before shifting to cloud. SLA should well define and document these security issues highlighted by Gartner and if considered appropriately it could provide an excellent base to standardize the SLA.

SLA for Cloud Security

The feasibility, efficiency, performance, and security of a cloud directly depend on the quality and the richness of SLA.

Confidentiality

As every Organization owns sensitive information it is necessary especially in an environment like cloud to ensure all means of information and transaction confidentiality to the organization to gain their trust. Their Information should be kept confidential by providing special controls over the information and applying restrictions on its access and disclosure. Customers should be informed for the confidentiality policy and plans and what encryption techniques or other methods are to be used to provide and ensure confidentiality in the cloud.

Integrity

It is important that the entire data going in and out of the cloud is made impossible to compromise. The customer should be assured of by keeping legality of their data. The cloud provider should guarantee and specify the procedures for the protection of data during the transit as well.

Availability

Availability is considered as the biggest advantage of cloud computing. SLA should have a fair amount of description on how the integrity targets are to be achieved in the cloud by mentioning how the threats to availability such as Virus attacks, Denial of Service Attacks, Hardware failure etc are to be identified, removed, managed and recovered.

Authenticity

The cloud provider as to ensure that the data, services, software etc provided to the customer are genuine. They also have to state who the customers will be and how they will be authenticated. The access control and privileges of those customers is also to be mentioned.

Non-repudiation

Auditing of the customers in the cloud should be made possible so that their actions can be traced and certified in a way that they can not decline their actions. The provider has to specify which method or encryption technique will be used to launch non-repudiation? And are the customers using the cloud able to reject their actions?

Privacy

Privacy is an important part of the customer's requirements. Privacy requirements should meet not only the needs of the customer but also comply with laws, standards, and service policies. (Miyazaki *et al*., 2008). The cloud provider should identify the data that is to be kept private in the cloud structure and also tell how the privacy of information of any entity belonging to the client's side will be protected.

Standards for Security Management

There are three Standards that are relevant to security management practices in the cloud. (Kresimir and Zeljko, 2010).

- Information Technology Infrastructure Library (ITIL)
- ISO/IEC 27001/27002
- Open Virtualization Format (OVF).

Information Technology Infrastructure Library (ITIL)

ITIL is an adaptable structure that contains a set of best practices and procedures to promote systematic and quality computing services in information technology. It is standardized in a series of books and was acknowledged by the UK Government's•Central Computer and Telecommunications Agency in the 1980's. ITIL can be applied across almost every type of IT environment including cloud operating environment (Mather *et al*., 2009). ITIL focus on all the aspects of IT service management and ensure that they are well defined and documented at the strategic, tactical and operational levels. It works as an iterative process for information security that must be controlled, planned, implemented, evaluated, and maintained. There are enormous advantages of adopting ITIL and if it is properly implemented the organizations can (The Benefits of ITIL, Web).

- Improve resource utilization.
- Be more competitive.
- Decrease rework.
- Eliminate redundant work.
- Improve upon project deliverables and time.
- Improve availability, reliability and security of mission critical IT services.
- Justify the cost of service quality.
- Provide services that meet business, customer and user demands.
- Integrate central processes.
- Document and communicate roles and responsibilities in service provision.
- Learn from previous experience.
- Provide demonstrable performance indicators.

ITIL focuses on information security in all of the IT services components of the organization. This will help the organization to avoid applying a sudden emergency state regarding information security on any service, and thus saving time and expenditures of the organization.

ITIL breaks information security into four different categories.(Mather *et al*., 2009).

- Policies: Overall objectives an organization is attempting to achieve
- Processes: What has to happen to achieve the objectives
- Procedures: Who does what and when to achieve the objectives
- Work instructions: Instructions for taking specific actions

The purpose of Security management is to guarantee the efficiency of information security and the basic goal of information

security is to ensure the protection of information. The protection of information can be achieved when it's Confidentiality, integrity, availability (CIA) and privacy requirements are fulfilled along with other objectives like Authenticity and Non-repudiation as mentioned earlier in the SLA for Cloud security.

ITIL has a separate process of operational guidance for security called the "ITIL Security Management Process" that specifies the adapted requirements of the organization regarding security controls which have been described in the SLA. It mainly describes the structural fitting of information security in the management organization, and•is based on the code of practice for information security management now known as•ISO/IEC 27002. (Wikipedia).

International Organization for Standardization (ISO) 27001/27002

ISO/IEC 27001 formally describes a management framework for the purpose of bring information security under defined management control. It specifies the main requirements for an Information Security Management System (ISMS).

ISO/IEC 27002 supplies code of practice on Information security management for the administrators in charge for initiating, implementing and maintaining ISMS.

Basically the ITIL along with ISO/IEC 20000, and ISO/IEC 27001/27002 frameworks help IT organizations internalize and respond to basic questions such as: (Mather *et al*., 2009)

"How do I ensure that the current security levels are appropriate for your needs"?

"How do I apply a security baseline throughout your operation"?

Simply to say, they help to respond to the question: "how do I ensure that my services are secure?"

Open Virtualization Format

Open Virtualization format (OVF) specifies a secure, efficient, portable, open and flexible format for the distribution of the enterprise software to Virtual machines. It provides an option for the customer to implement the OVF formatted virtual machine on any virtualization platform they like. OVF has significantly improved the customers' understanding with virtualization, by providing higher level of portability, platform independence, verification, signing, versioning, and licensing terms. OVF lets you (OVF, Web).

- Improve your user experience with streamlined installations.
- Offer customers virtualization platform independence and flexibility.
- Create complex pre-configured multi-tiered services more easily.
- Efficiently deliver enterprise software through portable virtual machines.
- Offer platform-specific enhancements and easier adoption of advances in virtualization through extensibility.

Advantage of Virtual appliances for cloud computing is that it does not require time to develop a system of applications with distributive features. Virtual appliances are being used in the majority of the cloud infrastructure because it gives an option to the cloud providers to mount it according to their requirements. Security and other application configurations become simpler to apply; as these open standard virtual appliances are coded in the form of XML description that could easily be modified.

ITIL Security Management

Cloud computing is mainly know for its dynamic characteristics and thus it becomes very complicated to manage the security processes for their effectiveness and to align them with the changing needs. For this reason the security management for a cloud environment should be continuous changeable to meet the altering security needs. A framework such as one provided by ITIL Security Management could be the best solution to this problem. ITIL Security Management process framework provides common, well-understood concepts and terminology so people clearly understand the reasons behind the security policies and procedures, as well as potential risk to the organization if they are not observed and followed (Security Manager, web). Its major role is to define the process of planning,

verify all the information of the organization, manage the defined level of information security, evaluate the risk factors, identify the economical preventive measures and define policies for access control.
The actions executed and controlled by Security Management are called Security Management Process. In cloud computing due to the reason mentioned earlier these processes must frequently be amended so that they can be valuable and fulfill the changing needs.
The goal of the Security Management is split up in two parts (Wikipedia).

Realization of security requirements

The security requirements are normally defined in the SLA and also in other external requirements, which are specified in underpinning contracts, legislation and possible internal or external imposed policies.

The realization of a basic level of security

This is necessary to guarantee the continuity of the organization and also necessary to reach a simplified service-level management for the information security, as it happens to be easier to manage a limited number of SLAs as it is to manage a large number of SLAs. SLA acts as a base and provides inputs for Security Management Process. These inputs are the requirements of the customers which are interpreted as security services that must be a part of the SLA for security. All the processes like Security Plans that contains Security Policies and Operation Level Agreements (OLA) are documented. OLA's are agreements that are developed internally within an organization to support the delivery of services to the customers. These security plans are then assessed and executed. Customers will have access to these reports so that they can know that their requirements getting fulfilled accordingly. Comparing these reports with the SLA the providers can also find more innovative ways to accurately assure that the have achieved the requirements.

ITIL Security Management Components

Due to the changing characteristics of cloud it is necessary for the activities of the security to repeatedly adjust according to the new requirements so that can they stay up dated and effective. ITIL security management is the perfect solution to cope with this problem. It has 5 processes used to control, plan, implement, evaluate and maintain the security processes. It is an iterative mechanism same as provide by the system development lifecycle models. The main advantage of ITIL security management is that it forms a formal document by reporting it at the end of each phase to both, the customer to check whether their needs are satisfied and the providers to check the status of security in different phases. The main components of ITIL security management process are:

Control

Control sub-process is the first step that control and organize ITIL Security Management process, defines the processes, assign tasks for the policy statement and the management of framework. In the control phase the security management framework defines the sub-processes for: (Wikipedia).

- The development of security plans.
- The implementation of the security plans.
- The evaluation and how the results of the evaluations are translated into action plans.
- Report to clients.

Sub-processes that take place in the Control process are (Wikpedia).

Implement policies

Policy Statement is the final product of this sub-process. A policy statement should contain the methods to generate measures for the security threats and to alert the organization prior to any security setback. These are detailed prerequisites and regulations that found the base for applying the security management process.

Setup the security organization

Security Management framework is the final

product of this sub-process. Security Management framework works as a structure that assembles security related information from different components within the organization for the purpose of analyzing and reporting it. Its main goal is to provide information security.

Reporting
In this sub-process entire control processes are documented is shape of a report.
A Control document is also maintained that has all the explanation of how security management process will be controlled and managed.

MATERIALS AND METHODS

The security part of the SLA is formed when the activities of the Plan sub-process are carried out according to the requirements of the customer mentioned in the SLA. This sub-process encompasses of some activities that are specially designed for supporting agreements that are necessary for security and lead to contracts detailed for security. The objectives defined in the SLA for security are originated as OLA. These OLA's Contain plans of security for organizational components. The Plan sub-process as to consider the policy statement described in the Control sub-process and also the requirements from SLA. Now ITIL process has to put its part so that these OLA's are properly managed and implemented. As told before that ITIL ensures the IT services are designed and documented on strategic, tactical and operational levels. The main role in plan sub-process will be played by operational level as it contains the following functions at are applicable over OLA's.

- Service Desk Management
- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management

Implementation
All the activities carried out in Plan sub-process needs to be well defined and evaluated, because they can not be changed in the implementation phase. After the successful completion of these activities in the Plan sub-process, their procedures are accurately implemented by Implementation sub-process.
The major activities of Implementation sub-process are to (Wikipedia).

I. Classify and manage IT applications
II. Implement Personnel security
III. Implement Security management
IV. Implement Access control

Evaluation
This sub-process reviews the validity and reliability of security plans and to ensure that it is rightly implemented. This can help both the provider and the customer to check the drawbacks of their system. It is helpful to ensure the customer that requirements mentioned in the SLA are getting exactly fulfilled. The Evaluation sub-process results can demand for change so it is launched back to the change management process of the ITIL. Basically there are three types of evaluation performed in the Evaluation sub-process.

Self Assessment
The implemented security agreements are tested here. Self assessment is performed over the process in the organization.

Internal Audit
This process is only concerned with the assessment of the implemented security agreements finalized internally in the organization by the internal IT auditors.

External audit
This process is only concerned with the assessment of the implemented security agreements finalized externally by independent IT auditors.
Apart from these evaluation types stated above another evaluation based on the security incidents is also taken in to consider. This evaluation focuses on the security events that are usually not considered in the normal course of operation but can be the basis to produce decline or

problem in the quality of the service.

Maintenance

Security Maintenance is an ongoing long term process. Organizations after implementing the accepted system do not give its required attention to its security. Security hazards are created with the change in the infrastructure of the system or within the organization. Maintenance sub process originates proposals from the outcomes of the evaluation sub process. These proposals will become the key for the activities in the Plan sub process. The change management process of ITIL will play a vital role to accommodate and control these new changes.

CONCLUSIONS

Cloud computing is still evolving and of course facing different problems, among which security is the critical one. It is costly and unsafe for organizations to carry out their own information security mechanisms for the complex and mounting security risks faced in the cloud, so there is a great need to follow a standardized and established approach such as ITIL. ITIL provides a standardized framework supported by best practices to offer any IT service including information security. ITIL security management process if followed properly could provide better explanation for information security as it can manage both the change and cost factors of the security threats faced in the cloud. The IaaS layer of cloud is the foundation for the structure of the cloud and the base for security processes so IaaS model should be develop according to ITIL guidelines. The main input for ITIL Security Management is SLA and the quality of service mainly depends on it. In this paper, we have suggested some techniques for the effective use of SLA and provided procedures for the information security using ITIL in the cloud which can decrease the security risks and hence increase availability of the cloud services whichwill raise the revenue for the organization in return using it.

REFERENCES

- Brodkin J. (2009). Gartner Seven cloud-computing security risks Data integrity, recovery, privacy and regulatory compliance are key issues to consider, Network World.
- Kandukuri BR, Paturi R and Rakshit R. “Cloud Security Issues”, International Institute of Information Technology Pune, India, 2009 IEEE International Conference on Services Computing.
- Kresimir P and Zeljko H. (2010) “Cloud computing security issues and challenges”, MIPRO 2010, May 24-28, Opatija, Croatia.
- Mather T,•Kumaraswamy S and•Laitf S. (2009). “Cloud security and privacy: *An Enterprise Perspective*• on Risks and Compliance”, *O'Reilly Media, Inc*.
- Miyazaki S, Mead N and Zhan J. (2008). “Computer-Aided Privacy Requirements Elicitation Technique” IEEE Asia-Pacific Services Computing Conference.
- Open Virtual Format, Virtual Appliances. http://www.vmware.com/appliances/getting-started/learn/ovf.html.
- SecurityManagement. http://www.teamquest.com/solutions/itil/security-management/index.htm.
- SLA Management Handbook. (2004). Enterprise Perspective. 4.
- The Benefits of ITIL, White Paper, http://www.peoplecert.org/en/ITIL_V3/ITIL_related_downloads/ITIL%20Brochures/ITIL_benefits.pdf.
- Wikipedia. http://en.wikipedia.org/wiki/ITIL_security_management.