The Impact Of Cloud Computing Technology On The Audit Process And The Audit Profession

Yati Nurhajati

Abstract: In the future, cloud computing audits will become increasingly, The use of that technology has influenced of the audit process and be a new challenge for both external and the Internal Auditors to understand IT and learn how to use cloud computing and cloud services that hire in cloud service provider (CSP), and considering the risks of cloud computing, and how to audit cloud computing by risk based audit approach. The wide range of unique risks and depend on the type and model of the cloud solution, the uniqueness of the client environment,and the specifics of data or an application make this an complicated subject. The internal audit function is well positioned through its role as a guarantor function of the organization to assist management and the board of the Committee to identify and consider the risks in using cloud computing technology for internal audit can help determine whether the risk has been managed appropriately in a cloud computing environment. Assesses the current impact of cloud computing technology on the audit process , and discusses the implications of cloud computing future technological trends for the auditing profession . More specifically, Provides a summary of how that information technology has impacted the audit framework.

Index Terms: Cloud service provider (CSP), Cloud Computing Environment, Risk Base`Audit approach, The Big Four Audit Firms, and Internal audit Role.

1. INTRODUCTION

In future years, cloud computing will become commonplace However, commercially available technology will continue to become less costly, and more widely available. The growth of enterprise-wide computing by virtual presents many new challenges for the audit. Demand of cloud computing is emerging when initially firms had to bear higly expensive cost for handling and maintenance all the computing resources and doubt to disclose their data to users. To overcome these problems Cloud Service Provider (CSP) providing management of physical resources, including computing resources , user data and sensitive process. Companies simply provide the data to the Cloud Service Provider (CSP) and further data will be accessible by anyone or user or any other company associated with Cloud Service Provider (CSP) or even every customer of the company itself. (Mohanty et al ; 2014) The Cloud supports a business model with some significant benefits for the consumer, including cost savings for equipment and for management of Information Technology (IT) resources and business services. But there are security risks exacerbated by outsourcing to the cloud that have not been fully understood by either buyers or Cloud Service provider (CSP), changes to IT infrastructure that are not understood by the business can introduce significant risk to the business itself, and so audit, compliance, and risk management should all be considered part of the true cost of cloud computing (Halpert, 2011; 15) Security of data into the most significant issues at all levels of Resource as a Service (RaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). At the network level, Cloud Service Provider (CSP) such as monitoring, collecting and firewall protection, perform intrusion prevention system and forwards the data stream.

- *Yati nurhajati, Student of Doctoral Program of Accounting Faculty of Economics and Business, Padjadjaran University- Bandung - Indonesia and Lecturer of LP3I - Bandung – Indonesia, E-mail nurhajatiyati@yahoo.co.id*

Hence auditing is highly required to maintain the privacy of the sensitive data, restricted access of computing and physical resources and to check integrity. (Mohanty et al, 2014). The purpose of this paper is to assess the current impact of cloud computing technology on the audit process, and to discuss the future implications of technological trends for the auditing profession. The paper first provides how cloud computing technology has impacted audit process are discussed. Next, provides a summary of the information gathered on the current usage of audit cloud computing technology by audit firms. The firms participating in this study represent two of the four largest accounting firms in the world.

2 LITERATURE REVIEW

2.1 HOW CLOUD COMPUTING TECHNOLOGY HAS IMPACTED AUDIT PROCESS

2.1.1 CLOUD COMPUTING

Cloud computing as a result of the collaboration of several existing technologies. (Halpert, 2011;2) when “the cloud” is combined with “computing,” Market research analysts and technology vendors alike tend to define cloud computing very narrowly, as a new type of utility computing that basically uses virtual servers that have been made available to third parties via the Internet. A more tempered view of cloud computing considers it the delivery of computational resources from a location other than the one from which you are computing. (Ransome and Rittinghouse, 2010; xxvii) National Institute of Standards and Technology (NIST) at NIST Special Publication 800-145 (2011), defines ”Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of three service models, and four deployment models as follow; The NIST Special Publication 800-145 (2011) also identifies three cloud service models and four cloud deployment models.

The service models are:

1. Software-as-a-Service (SaaS) allows users to run a variety of software applications on the Internet without having possession or managing applications (e.g., Salesforce.com, Gmail, Microsoft Online).
2. Platform-as-a-Service (PaaS) provides a computing platform to support building of web applications and services completely residing on the Internet (e.g., Google Apps, Force.com, 3Tera AppLogic).
3. Infrastructure-as-a-Service (IaaS) allows the use of computer hardware and system software, including operating systems and communication networks in which the cloud provider is responsible for hardware installation, system configuration, and maintenance (e.g., Amazon EC2, Citrix Cloud Center).

The Deployment Models are:

1. Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2. Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
3. Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
4. Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

2.1.2 AUDITING IN CLOUD COMPUTING ENVIRONMENT

According to Halpert (2011) The best practice in effective IT auditing is to start with an understanding of business functions, to identify which IT infrastructure is providing those functions, and to then consider the scope of the audit and controls best suited for that IT function. Similarity and diferrence of auditing at cloud computing environment:

a. Audit in the cloud does have similar issues to standard infrastructure auditing that should be considered, as follow ;

- conflict of interest and independence of the auditor
- professional auditing practices and adequate technical training and proficiency of the auditor
- audit reports that clearly assert findings and qualified opinions-based evidence and documentation.

b. Audit will be different for the cloud depending on ;

- the deployment model of cloud outsourcing (private, public, community, or hybrid) and service model Software as a Service [SaaS]

Example:

The essential differences will be most evident in the public and hybrid types of clouds—as these will rely most heavily on contracts and (possibly complex) agreements and compliance to those agreements.

- The service model Software as a Service [SaaS], Infrastructure as a Service [IaaS], Platform as a Service [PaaS].
- The use of the cloud implies the use of the Internet and ‘‘extension’’ of the corporate network, all cloud models vary in features and controls that must be considered while planning and executing an audit.

2.1.2 STANDAR FRAMEWORK CONTROL TO CLOUD COMPUTING ENVIRONMENT

Control (compliance) frameworks have not yet been well adapted to cloud environments, although most (like COBIT, ITIL, and ISO 27001) are considered sufficient overall and a worthy starting point. Information assurance controls or Common Criteria have supported auditing by dictating minimal requirements for audit. CSA, NIST, ISACA, and ENISA. These organizations have been leading the development of concepts and guidance sufficient to understand, protect, and trust cloud infrastructure. It is advisable to keep up with new publications from these organizations (and many others) to keep abreast of new thought and advice. .(Halpert, 2011; 19)

2.1.3 AUDIT RISK BASED APPROACH IN CLOUD COMPUTING ENVIRONMENT AND INTERNAL AUDITOR ROLE

Process auditing has become much more important as an auditor must begin the audit planning by understanding the objectives of each business process and then determine whether these objectives have been incorporated into the client's processes, while adequately considering risks and internal controls(Bierstaker et al, 2001). According to Halpert (2011;27) An auditor should be able to review the risk assessment product and observe the risk assessment process. Singleton (2010) propose a risk-based approach that encourages effective risk assessment and auditing for the identified risks. The very best Internal Audit functions are regarded as a catalyst for change, helping the organisation through the difficulties of changing environments, cultures, and so on. (Phil Griffiths (2005;8) So IT auditors need to understand these technologies, establish an approach for identifying the key risks and develop effectual audits of the technologies for those risks. However, the risk-based approach (RBA) process for cloud computing is complicated by the fact that all of the technologies and controls are housed outside the entity being audited (Singleton, 2010). The cloud user is strongly advised to perform a risk assessment of any system proposed for the cloud environment. In some cases, the assessment of risk will be performed as part of enterprise risk management and should be adjusted to address specific risks associated with different vendors, specific cloud offerings, existing compliance requirements, and data sensitivity. The wide range of unique risks facing the organization make this an important subject and depend on the type and model of the cloud solution, the uniqueness of the client environment,and the specifics of data or an application (Halpert, 2011;26-27)

2.1.4 AUDITING FRAMEWORK IN CLOUD COMPUTING ENVIRONMENT

2.1.4.1 AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS ARE INFRASTRUCTURE AS A SERVICE (IAAS) AND SOFTWARE AS A SERVICE (SAAS)

Singleton (2010) asserts that IT auditors need to understand cloud technology, especially SaaS and IaaS; establish an approach for identifying key risks; and develop effective audits. There is a simple framework for thinking about cloud computing that should help IT auditors in performing a risk assessment. The components are Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—almost identical to the way we think of the body of technologies internal to an entity

A. AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS INFRASTRUCTURE AS A SERVICE (IAAS)

Services of IaaS components replace or supplement the internal infrastructure. The key decision factors for management in deciding to move to IaaS (outsourcing part of its infrastructure) and choosing the appropriate vendor are usually efficiency-related.There are various ways to break down IaaS, but here is one way:

1) Connectivity
2) Network services and management
3) Compute services and management
4) Data storage
5) Security

1. Connectivity obviously refers to reliable access to the Internet and connectivity to associated systems and technologies, for instance, data storage to application servers. Examples of risks would be availability/downtime and speed of access.
2. Network services and management includes not only providing network capabilities, but managing the network, monitoring the network and providing for efficient access through aspects such as load balancing. Examples of these risks scalability for new technologies or expanding the level of transactions, availability, secured transmissions, and the level of access (e.g., load balancing).
3. Compute services and management include appropriate resources such as core, processors, memory and managing the operating system (OS). Examples of the risks are availability (including system failure) and scalability.
4. There has been significant growth in data centers over the last few years, and data centers are becoming more sophisticated in the scope of services. Examples of the risks for data storage include the obvious: security of data, recovery, availability and scalability.
5. The security and recovery issues are particularly important. Management should ensure that the data storage aspect of IaaS can provide an appropriate level of physical and logical security and an appropriate recovery methodology to ensure a timely recovery if the data center is involved in a disaster.

B. AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS SOFTWARE AS A SERVICE (SAAS)

Some of the key points in deciding to use SaaS, or a particular vendor, are the complexity of the environment, the need to buy smaller pieces/modules, compatibility with existing systems and IT (including programming platform), ease of purchase, ease of integration, project management, scalable infrastructure, and billing/costs (metering). There are various ways to break down SaaS, but here is one framework:

a. Business process modeling ; involves the need to fit together workflow/business process structure, applications and data, organizational structure, and the integration of existing systems.
b. Evaluation and analysis ; Evaluation and analysis includes process cost accounting, balanced scorecards, service level agreements (SLA), process warehouse and optimization.
c. Process execution; Process execution includes workflow control, applications integration (enterprise application integration [EAI]), service orchestration (service-oriented architecture [SOA]), populating databases/conversion and business activity monitoring.

2.1.4.2 AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON CLOUD AUDITING OUTSOURCING LIFECYCLE FASE

Mohanty, pattnaik, and mund (2014) state auditing is needed in every phases of cloud infrastructure due to maintenance of data confidentiality, privacy, integrity and availability. In the recent scenario, data is being stored, transferred and processed outside the company or organization. Organizations outsourced all its sensitive data, processes and computing resources to the Third Party Vendor for handling and maintenance of those data and resources, it is going through different phases as follows: Phase 1 Selecting the appropriate Third Party vendor: When an organization wants to deploy its application or want to rent the physical resources or need an independent platform where heterogeneous application can be executed, it needs to select the proper vendor which should be able to handle all the requirements. Phase 2 Define strategy: The service provider vendor should be transparent in defining its business strategy and risk management philosophy. This kind of decision strategy will enable the service provider to meet the baseline requirements of its consumers. Phase 3 Define policies and workflow: Having defined its strategy and customer-requirements, service provider needs to translate its requirements into policies applicable to industry standards. In this phase, providers need to determine the configuration settings, flow control, platforms and to maintain the workflow. Phase 4 Establishing business case: Driven by the strategy and policies of the service provider, the business case is established and different concerns related to privacy, security and availability should be in the business protocol Phase 5 Due diligence of the Third Party Vendor: An act with a firm standard of care should be established within the Third Party Service Provider. Due diligence process is being concerned with some issues like Compatibility audit, Marketing audit,financial audit, Management audit, Legal audit, and Information systems audit. The technological direction of both the Third Party and the concerned organization should the directly aligned. Phase 6 Validating Agreement protocol and establishing relationships: A Service Level Agreement (SLA) protocol and escrow service are being established between both vendor and the organization so that both can meet in a standardize platform. Both should know the responsible authorities with their functionalities. Phase 7 Dynamic monitoring: In this phase of lifecycle, dynamic monitoring service is getting enabled and dynamically monitors whether the vendor can continue the stable operations, can provide services or not. In the

meanwhile, Auditors are actively maintaining the privacy of the sensitive data and computing resources and preparing independent auditor's report. Phase 8 Closing the relationship: In last phase of the cycle, data is transferred and unused data are cleaned up. Acknowledgement message is also transferred from the user and even related organization end. And the concerned vendor will be getting ready for the next transaction.

Mohanty, pattnaik, and mund (2014) propose The auditing aspects in Cloud Computing Environment are discussed as follows:

1. Auditing for regulation or compliance: A set of rules and principles are designed to govern or control the conduct for auditing. Compliance is concerned with legal issues, social activities, marketing strategies, and co-operative conduct. In every aspects of compliance, auditing is highly needed for maintenance of governing conduct. Auditing for regulations and compliance is also needed to restrict increasing complexity to comply with standards and to maintain the agreement for privacy laws.
2. Auditing for Risk and Governance: Governance is exceedingly concerned with the performance measurement & its strategies and risk management & its proper administration is also an important issue of an IT landscape. Different management laws and policies, priority & resources needed for the processes, alignment of customs are the basic functionalities of this category.
3. Auditing for security: Security issues are the concern for auditing. In the administration security, everyone should know the responsibilities of each designation. Technical auditing is also concerned with security issues. Physical resources are also in need of auditing for its priority, availability and cost complexity.
4. Database Auditing: Database auditing is related with observing a cloud database so as database auditors and administrators can take care of the actions like accesses, modifications, updating issue of the database users. Database auditing is mainly query-based auditing. Queries are presented to the auditor one at a time; auditor checks if answering the query combining with past answers reveals the secret or forbidden information.
5. Service level agreements (SLAs) Auditing: In Business Service Provider (BSP) layer, SLAs is concerned about business-oriented agreement and laws. So in every level of agreements, auditing is highly required to maintain to proper usage of laws and terms & conditions.
6. Third Party Storage Auditing Service Provider: Considering Cloud data storage and database service, four different entities are there in Third Party Storage Auditing Service Provider, as shown in the [Figure1]: The Cloud user, hosting machine in Cloud Service Provider (CSP), Cloud Database Server (CDS) and Third Party Auditing Service (TPAS). The cloud user, having a huge amount of data files which is to be stored in the cloud. The Cloud user interacts with hosting machine in CSP through Cloud-based user Interface and deploys various applications. They may also dynamically communicate with Cloud Database Server (CDS) for storing and maintenance of their data files. While deploying their various applications onto host machine, the users may rely on TPAS in assuring the confidentiality, availability and integrity of their outsourced data to preserve the privacy of their own data. TPAS is capable of maintaining the privacy of user-data and can be trusted as it may review the cloud database storage reliability in support of the cloud user upon request. An unauthorized user can put a set of intelligent queries to the database server, of which none of the query is forbidden. So the unauthorized user, combining the set of replies, may get the secret information which is forbidden. Hence TPAS has the responsibility to maintain the privacy of user data.

2.3 Audit cloud computing technology by The Big Four audit firms

The Big four is the four largest accounting firms that handle accounting services for a number of public and private companies. The Big Four includes Deloitte Touche Tohmatsu, Pricewaterhousecoopers, Ernst & Young, and KPMG. The Big Four was formed in 2002 after a series of mergers, including the collapse of Enron, reduced the original eight down to four For how are the big four audit performing Risk based audit approach in cloud computing envionmental in this paper. The firms participating in this study represent two of the four largest audit firms consist of KPMG and Deloitte.

2.1.4.3 How are the Big Four to audit with risk-based audit approach on cloud computing environment

A. DELOITTE

In Deloitte presentation (2014) entitled "Cloud Computing - What Auditors need to know ". Explaining the risks and control company's that move to cloud , cloud effect on Auditing , and its influence on the internal auditor's role , how to manage risks , and solutions based on the risk-based approach Deloitte, (2014) states that Cloud computing is a challenge for Auditing ,

a. A disruptive technology, like cloud computing, can impact "how" to audit.
b. Internal audit and compliance have a key role to play in helping to manage and assess risk as cloud services evolve, especially for third-party compliance"
c. Deloitte asserts that understanding the various cloud models by risk based approach will help manage risk. that by understanding the various threats on cloud models used to approach Risk-based Approach will help to manage risk
d. Deloitte (2014) propose Tools and dan framework standar, as follow:

- Standar framework controlnya menggunakan NIST SP 800-53, NIST SP 800-144, SP 800-30
- Deloitte untuk membantu proses auditnya dengan membuat Deloitte Cloud Computing Risk Intelligence Map dan Cloud Security Alliance - Cloud Controls Matrix

e. Developing audit base risk approach the name is Deloitte's Cloud Computing Risk Intelligence Map

Use and Benefits

–Identifies significant risks that may be introduced by cloud computing

–Expands the risk discussion to the broad range of risks that need to be considered across the enterprise

f. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

It provides a controls framework is aligned to the Cloud Security Alliance guidance in 16 domains.
• The foundations rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP
• It will augment or provide internal control direction for SOC attestations provided by cloud providers.

Based on the above understanding can be concluded that Deloitte conducted audits based on risk by developing the technique itself is Deloitte's Cloud Computing Risk Intelligence Map, and consider the role of internal audit and to help manage and assess the risks of cloud services is growing, it indicates that an auditor in auditing the cloud should understand IT well .

A.KPMG
KPMG in the exposure of "Cloud Computing An Internal Audit Perspective" at the Institute of Internal Auditors Topeka Chapter December 6, 2011 KPMG suggests internal auditor to conduct an audit in a cloud computing environment with the relationship between risk takes from every phase in the Cloud Outsourcing Lifec

Risk Related Considerations for Each Phase:
Phase 1 – Establishing business case
•Is the work core to the organization's business?
•Are there over-riding concerns related to security, privacy, and availability given the nature of the business?
Phase 2 – Vendor due diligence
•Does the technological direction of vendor align with the user organization's direction?
• Is the vendor stable from a finance and operations perspective?
Phase 3 – Establishing vendor relationships
•Are there service-level agreements and escrow?
•Do you know who is responsible for what'?
Phase 4 – Ongoing monitoring
•Does the vendor continue to operate with stability?
•independent auditor's report?
•Is there an auditor s
Phase 5 – Closing the relationship
•Data transfer and clean up
•Knowledge transfer

KPMG (2013) in the exposure of "the Cloud Computing : Risks and Auditing". IIA Chicago Chapter 53rdAnnual Seminar . April 15, 2013 to explain how the cloud computing division of the dimensions of risk and consideration of the audit of the risk. KPMG share risks in cloud computing environments in several dimensions as follow ; Here is a cloud computing audit in five areas deemed relevant KPMG :
1. Data Protection
2. Risk Technology
3. Identity and Access Management
4. rules
5. Operation

According to Halpert (2011) The best practice in effective IT auditing is to start with an understanding of business functions, to identify which IT infrastructure is providing those functions, and to then consider the scope of the audit and controls best suited for that IT function. Similarity and diferrence of auditing at cloud computing environment:
a. Audit in the cloud does have similar issues to standard infrastructure auditing that should be considered, as follow ;
- conflict of interest and independence of the auditor
- professional auditing practices and adequate technical training and proficiency of the auditor
- audit reports that clearly assert findings and qualified opinions-based evidence and documentation.

b. Audit will be different for the cloud depending on ;
- the deployment model of cloud outsourcing (private, public, community, or hybrid) and service model Software as a Service [SaaS]

Example:
The essential differences will be most evident in the public and hybrid types of clouds—as these will rely most heavily on contracts and (possibly complex) agreements and compliance to those agreements.
• The service model Software as a Service [SaaS], Infrastructure as a Service [IaaS], Platform as a Service [PaaS].

The use of the cloud implies the use of the Internet and ''extension'' of the corporate network, all cloud models vary in features and controls that must be considered while planning and executing an audit.

2.1.5 STANDAR FRAMEWORK CONTROL TO CLOUD COMPUTING ENVIRONMENT

Control (compliance) frameworks have not yet been well adapted to cloud environments, although most (like COBIT, ITIL, and ISO 27001) are considered sufficient overall and a worthy starting point. Information assurance controls or Common Criteria have supported auditing by dictating minimal requirements for audit. CSA, NIST, ISACA, and ENISA. These organizations have been leading the development of concepts and guidance sufficient to understand, protect, and trust cloud infrastructure. It is advisable to keep up with new publications from these organizations (and many others) to keep abreast of new thought and advice. .(Halpert, 2011; 19)

2.1.6 AUDIT RISK BASED APPROACH IN CLOUD COMPUTING ENVIRONMENT AND INTERNAL AUDITOR ROLE

Process auditing has become much more important as an auditor must begin the audit planning by understanding the objectives of each business process and then determine whether these objectives have been incorporated into the client's processes, while adequately considering risks and internal controls(Bierstaker et al, 2001). According to Halpert (2011;27) An auditor should be able to review the risk assessment product and observe the risk assessment process. Singleton (2010) propose a risk-based approach that encourages effective risk assessment and auditing for the identified risks. The very best Internal Audit functions are regarded as a catalyst for change, helping the organisation through the difficulties of changing environments, cultures, and so on. (Phil Griffiths (2005;8) So IT auditors need to understand these technologies, establish an approach for identifying the key risks and develop effectual audits of the technologies for those risks. However, the risk-based approach (RBA) process for cloud computing is complicated

by the fact that all of the technologies and controls are housed outside the entity being audited (Singleton, 2010). The cloud user is strongly advised to perform a risk assessment of any system proposed for the cloud environment. In some cases, the assessment of risk will be performed as part of enterprise risk management and should be adjusted to address specific risks associated with different vendors, specific cloud offerings, existing compliance requirements, and data sensitivity. The wide range of unique risks facing the organization make this an important subject and depend on the type and model of the cloud solution, the uniqueness of the client environment,and the specifics of data or an application (Halpert, 2011;26-27)

2.1.7 AUDITING FRAMEWORK IN CLOUD COMPUTING ENVIRONMENT

2.1.7.1 AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS ARE INFRASTRUCTURE AS A SERVICE (IAAS) AND SOFTWARE AS A SERVICE (SAAS)

Singleton (2010) asserts that IT auditors need to understand cloud technology, especially SaaS and IaaS; establish an approach for identifying key risks; and develop effective audits. There is a simple framework for thinking about cloud computing that should help IT auditors in performing a risk assessment. The components are Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—almost identical to the way we think of the body of technologies internal to an entity

C. AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS INFRASTRUCTURE AS A SERVICE (IAAS)

Services of IaaS components replace or supplement the internal infrastructure. The key decision factors for management in deciding to move to IaaS (outsourcing part of its infrastructure) and choosing the appropriate vendor are usually efficiency-related. There are various ways to break down IaaS, but here is one way:

1. Connectivity
2. Network services and management
3. Compute services and management
4. Data storage
5. Security

1. Connectivity obviously refers to reliable access to the Internet and connectivity to associated systems and technologies, for instance, data storage to application servers. Examples of risks would be availability/downtime and speed of access.
2. Network services and management includes not only providing network capabilities, but managing the network, monitoring the network and providing for efficient access through aspects such as load balancing. Examples of these risks scalability for new technologies or expanding the level of transactions, availability, secured transmissions, and the level of access (e.g., load balancing).
3. Compute services and management include appropriate resources such as core, processors, memory and managing the operating system (OS). Examples of the risks are availability (including system failure) and scalability.
4. There has been significant growth in data centers over the last few years, and data centers are becoming more sophisticated in the scope of services. Examples of the risks for data storage include the obvious: security of data, recovery, availability and scalability.
5. The security and recovery issues are particularly important. Management should ensure that the data storage aspect of IaaS can provide an appropriate level of physical and logical security and an appropriate recovery methodology to ensure a timely recovery if the data center is involved in a disaster.

D. AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON THE COMPONENTS SOFTWARE AS A SERVICE (SAAS)

Some of the key points in deciding to use SaaS, or a particular vendor, are the complexity of the environment, the need to buy smaller pieces/modules, compatibility with existing systems and IT (including programming platform), ease of purchase, ease of integration, project management, scalable infrastructure, and billing/costs (metering). There are various ways to break down SaaS, but here is one framework:

1. Business process modeling ; involves the need to fit together workflow/business process structure, applications and data, organizational structure, and the integration of existing systems.
2. Evaluation and analysis ; Evaluation and analysis includes process cost accounting, balanced scorecards, service level agreements (SLA), process warehouse and optimization.
3. Process execution; Process execution includes workflow control, applications integration (enterprise application integration [EAI]), service orchestration (service-oriented architecture [SOA]), populating databases/conversion and business activity monitoring.

2.1.7.2 AUDITING CLOUD COMPUTING FRAMEWORK IN PERFORMING A RISK ASSESSMENT BASE ON CLOUD AUDITING OUTSOURCING LIFECYCLE FASE

Mohanty, pattnaik, and mund (2014) state auditing is needed in every phases of cloud infrastructure due to maintenance of data confidentiality, privacy, integrity and availability. In the recent scenario, data is being stored, transferred and processed outside the company or organization. Organizations outsourced all its sensitive data, processes and computing resources to the Third Party Vendor for handling and maintenance of those data and resources, it is going through different phases as follows:

Phase 1 Selecting the appropriate Third Party vendor: When an organization wants to deploy its application or want to rent the physical resources or need an independent platform where heterogeneous application can be executed, it needs to select the proper vendor which should be able to handle all the requirements.

Phase 2 Define strategy: The service provider vendor should be transparent in defining its business strategy and risk management philosophy. This kind of decision strategy will enable the service provider to meet the baseline requirements of its consumers.

Phase 3 Define policies and workflow: Having defined its strategy and customer-requirements, service provider needs to translate its requirements into policies applicable to industry standards. In this phase, providers need to determine the configuration settings, flow control, platforms and to maintain the workflow.

Phase 4 Establishing business case: Driven by the strategy and policies of the service provider, the business case is established and different concerns related to privacy, security and availability should be in the business protocol

Phase 5 Due diligence of the Third Party Vendor: An act with a firm standard of care should be established within the Third Party Service Provider. Due diligence process is being concerned with some issues like Compatibility audit, Marketing audit,financial audit, Management audit, Legal audit, and Information systems audit. The technological direction of both the Third Party and the concerned organization should the directly aligned.

Phase 6 Validating Agreement protocol and establishing relationships: A Service Level Agreement (SLA) protocol and escrow service are being established between both vendor and the organization so that both can meet in a standardize platform. Both should know the responsible authorities with their functionalities.

Phase 7 Dynamic monitoring: In this phase of lifecycle, dynamic monitoring service is getting enabled and dynamically monitors whether the vendor can continue the stable operations, can provide services or not. In the meanwhile, Auditors are actively maintaining the privacy of the sensitive data and computing resources and preparing independent auditor's report.

Phase 8 Closing the relationship: In last phase of the cycle, data is transferred and unused data are cleaned up. Acknowledgement message is also transferred from the user and even related organization end. And the concerned vendor will be getting ready for the next transaction.

Mohanty, pattnaik, and mund (2014) propose The auditing aspects in Cloud Computing Environment are discussed as follows:

1. Auditing for regulation or compliance: A set of rules and principles are designed to govern or control the conduct for auditing. Compliance is concerned with legal issues, social activities, marketing strategies, and co-operative conduct. In every aspects of compliance, auditing is highly needed for maintenance of governing conduct. Auditing for regulations and compliance is also needed to restrict increasing complexity to comply with standards and to maintain the agreement for privacy laws.
2. Auditing for Risk and Governance: Governance is exceedingly concerned with the performance measurement & its strategies and risk management & its proper administration is also an important issue of an IT landscape. Different management laws and policies, priority & resources needed for the processes, alignment of customs are the basic functionalities of this category.
3. Auditing for security: Security issues are the concern for auditing. In the administration security, everyone should know the responsibilities of each designation. Technical auditing is also concerned with security issues. Physical resources are also in need of auditing for its priority, availability and cost complexity.
4. Database Auditing: Database auditing is related with observing a cloud database so as database auditors and administrators can take care of the actions like accesses, modifications, updating issue of the database users. Database auditing is mainly query-based auditing. Queries are presented to the auditor one at a time; auditor checks if answering the query combining with past answers reveals the secret or forbidden information.
5. Service level agreements (SLAs) Auditing: In Business Service Provider (BSP) layer, SLAs is concerned about business-oriented agreement and laws. So in every level of agreements, auditing is highly required to maintain to proper usage of laws and terms & conditions.
6. Third Party Storage Auditing Service Provider: Considering Cloud data storage and database service, four different entities are there in Third Party Storage Auditing Service Provider, as shown in the [Figure1]: The Cloud user, hosting machine in Cloud Service Provider (CSP), Cloud Database Server (CDS) and Third Party Auditing Service (TPAS). The cloud user, having a huge amount of data files which is to be stored in the cloud. The Cloud user interacts with hosting machine in CSP through Cloud-based user Interface and deploys various applications. They may also dynamically communicate with Cloud Database Server (CDS) for storing and maintenance of their data files. While deploying their various applications onto host machine, the users may rely on TPAS in assuring the confidentiality, availability and integrity of their outsourced data to preserve the privacy of their own data. TPAS is capable of maintaining the privacy of user-data and can be trusted as it may review the cloud database storage reliability in support of the cloud user upon request. An unauthorized user can put a set of intelligent queries to the database server, of which none of the query is forbidden. So the unauthorized user, combining the set of replies, may get the secret information which is forbidden. Hence TPAS has the responsibility to maintain the privacy of user data.

2.3 Audit cloud computing technology by The Big Four audit firms

The Big four is the four largest accounting firms that handle accounting services for a number of public and private companies. The Big Four includes Deloitte Touche Tohmatsu, Pricewaterhousecoopers, Ernst & Young, and KPMG. The Big Four was formed in 2002 after a series of mergers, including the collapse of Enron, reduced the original eight down to four For how are the big four audit performing Risk based audit approach in cloud computing envionmental in this paper. The firms participating in this study represent two of the four largest audit firms consist of KPMG and Deloitte.

2.3.1 How are the Big Four to audit with risk-based audit approach on cloud computing environment

DELOITTE

In Deloitte presentation (2014) entitled "Cloud Computing - What Auditors need to know ". Explaining the risks and control company's that move to cloud , cloud effect on Auditing , and

its influence on the internal auditor's role , how to manage risks , and solutions based on the risk-based approach Deloitte, (2014) states that Cloud computing is a challenge for Auditing ,

a. A disruptive technology, like cloud computing, can impact "how" to audit.
b. Internal audit and compliance have a key role to play in helping to manage and assess risk as cloud services evolve, especially for third-party compliance"
c. Deloitte asserts that understanding the various cloud models by risk based approach will help manage risk. that by understanding the various threats on cloud models used to approach Risk-based Approach will help to manage risk

c. Deloitte (2014) propose Tools and dan framework standar, as follow:

- Standar framework controlnya menggunakan NIST SP 800-53, NIST SP 800-144, SP 800-30
- Deloitte untuk membantu proses auditnya dengan membuat Deloitte Cloud Computing Risk Intelligence Map dan Cloud Security Alliance - Cloud Controls Matrix

d. Developing audit base risk approach the name is Deloitte's Cloud Computing Risk Intelligence Map

Use and Benefits

i. Identifies significant risks that may be introduced by cloud computing
ii. Expands the risk discussion to the broad range of risks that need to be considered across the enterprise

e. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

It provides a controls framework is aligned to the Cloud Security Alliance guidance in 16 domains.

1. The foundations rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP
2. It will augment or provide internal control direction for SOC attestations provided by cloud providers. Based on the above understanding can be concluded that Deloitte conducted audits based on risk by developing the technique itself is Deloitte 's Cloud Computing Risk Intelligence Map, and consider the role of internal audit and to help manage and assess the risks of cloud services is growing, it indicates that an auditor in auditing the cloud should understand IT well .

KPMG

KPMG in the exposure of "Cloud Computing An Internal Audit Perspective" at the Institute of Internal Auditors Topeka Chapter December 6, 2011 KPMG suggests internal auditor to conduct an audit in a cloud computing environment with the relationship between risk takes from every phase in the Cloud Outsourcing Lifec

Risk Related Considerations for Each Phase:

Phase 1 – Establishing business case

- Is the work core to the organization's business?
- Are there over-riding concerns related to security, privacy, and availability given the nature of the business?

Phase 2 – Vendor due diligence

- Does the technological direction of vendor align with the user organization's direction?
- Is the vendor stable from a finance and operations perspective?

Phase 3 – Establishing vendor relationships

- Are there service-level agreements and escrow?
- Do you know who is responsible for what'?

Phase 4 – Ongoing monitoring

- Does the vendor continue to operate with stability?
- independent auditor's report?
- Is there an auditor s

Phase 5 – Closing the relationship

- Data transfer and clean up
- Knowledge transfer

KPMG (2013) in the exposure of "the Cloud Computing : Risks and Auditing". IIA Chicago Chapter 53rdAnnual Seminar . April 15, 2013 to explain how the cloud computing division of the dimensions of risk and consideration of the audit of the risk. KPMG share risks in cloud computing environments in several dimensions as follow ;

Here is a cloud computing audit in five areas deemed relevant KPMG:

1. Data Protection
2. Risk Technology
3. Identity and Access Management
4. rules
5. Operation

4 CONCLUSION

Audit in a cloud environment is a combination of information systems audit and audit of Information Technology (audit of infrastructure IT). Understanding the process of auditing in cloud computing environments with knowing there was have two audit site consist of audit on-site service cloud provider (CSP) and audit at the company's site (costumer cloud service). the risk-based approach (RBA) process for cloud computing is complicated because the technologies and controls are housed outside the entity being audited and unfortunally Standard framework audit control cloud computing is still in development. From the above problems Clearly we could find there was differences in the Auditing framework that conducted each audit firms, They are makes Cloud computing superior risk intelligence maps that basically using Risk-based audit approach. Cloud computing is a technology that is predicted to continue to grow so, will be crucial in the coming years , An auditor should be able to review the risk assessment products and observe the process of risk assessment. While the role of internal auditors is crucial in developing additional understanding of this new technology to add value and more to advise their companies on the relevant risks and controls, as internal auditors have a higher level of understanding of Business Processes and operational audit

ACKNOWLEDGMENT

I thank an reviewer Prof. Dr. Azhar Susanto, PGDBus., SE., Ak., CPA., CA. and all participants at my Information System Auting class in DIA Unpad for the helpful suggestions and comments on earlier drafts of this paper. Financial support from LP3I is gratefully acknowledged.

REFERENCES

[1] Arens, Alvin, A., Elder, Randal J. and Beasley , Mark S. 2012. Auditing and Assurance Services An Integrated Approach. International Edition, Fourth Edition. New Jersey: Pearson Prentice-Hall Inc.

[2] Becker, Jack D. & Elana Bailey. 2014. IT Controls and Governance in Cloud Computing. AMCIS Proceedings forthcoming

[3] Bierstaker , James L. , Priscilla Burnaby and Jay Thibodeau. 2001. The Impact of Information Technology on the audit Process: an assessment of the state of the art andimplications for the future. Managerial Auditing Journal, 16/3 [2001] 159-164

[4] Deloitte (2014). Cloud Computing –What Auditors need to . Retrieved from http://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/10-14-16-cloud-computing/cloudcomputing.pdf

[5] Griffiths, Phil. 2005. Risk-based auditing. Burlington USA. Gower Publishing Company.

[6] Halpert, Ben. 2011. Auditing Cloud Computing A Security and Privacy Guide.john Wiley & Sons, Inc. Hoboken, New Jersey. Canada.

[7] Lageschulte, Phil & Sailesh Gadia.. 2013. Cloud Computing: Risks and Auditing in IIA Chicago Chapter 53rdAnnual Seminar. Convention Center. KPMG. USA. Retrieved from

[8] Wieger, Partner

[9] Madhav Panwar. 2013. Special Cloud Computing Guide & Handbook. SAI. U.S.A.

[10] Messier, William F. 2008. Auditing & assurance services: a systematic approach, Fifth Edition. New JerseyYork. McGraw-Hill Companies.

[11] Mell, Peter and Timothy Grance. 2011. Special Publication 800-145. Departement of Commerce National Institute of Standards and Technology (NIST). U.S.

[12] Mell, Peter and Timothy Grance. 2011. Special Publication 800-145. Departement of Commerce National Institute of Standards and Technology (NIST). U.S.

[13] Mohanty, suneeta., prasant kumar pattnaik, and ganga bishnu mund. 2014. framework for auditing in cloud computing environment. Journal of Theoretical and Applied Information Technology.

[14] Lageschulte, Phil. and Sailesh Gadia (KPMG). 2013. Cloud Computing: Risks and Auditing. IIA Chicago Chapter 53rdAnnual Seminar. April 15, 2013, Donald E. Stephens Convention Center. Retrieved from ; https://chapters.theiia.org/chicago/Annual%20Seminar%20Presentations/E3%20-%20Cloud%20Computing%20Risks%20and%20Auditing.pdf

[15] Ransome, James F., and John W. Rittinghouse. 2010. Cloud Computing Implementation, Management, and Security . Boca Raton London New York. Gower Publishing Company.