https://doi.org/10.46335/IJIES.2022.7.9.14 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 68-70

International Journal of Innovations in Engineering and Science, www.ijies.net

Risk Analysis and Comparative Study of the Different Cloud Computing Providers in India

Mohini.M.Hadap[1] , Dr. Madhura Chinchamalatpure[2]

G. H. Raisoni Institute of Engineering and Technology, Nagpur

mohini.hadap99@gmail.com

***Received on**: 11 June ,2022* ***Revised on**: 07 August ,2022,* ***Published on**: 09 August,2022*

***Abstract –** The objective of this research is to evaluate the risk of cloud computing in India. Risk assessment is conducted on the system and recommendation of control is provided to help cloud provider in India to reduce risks. The assessment result should increase level of awareness to threats in cloud environment and help consumers to choose the right cloud providers. At the end, this paper can be used as a guide for Indian government to prepare the required infrastructure by cloud providers to run their business in India.*

***Keywords**— Cloud computing, Cloud security, Risk assessment, Data center, RIIOT, CS Aguide.*

I - INTRODUCTION

With the technology advances, businesses also need to keep up with the existing technology to provide real business solutions. To maintain the business competitive edge, businesses need to continuously find ways to reduce costs and one of the emerging solutions is to migrate to cloud [1], where “about 500crores could be saved annually by moving to cloud networks". From the business perspective, cloud computing becomes one of the key technologies that provide real promise to business with real cost-cutting and computational power [2]. In general, there are 3 major services that cloud computing provide: Infrastructure as a Service (IaaS), Platform as a service (PaaS) and Software as a Services (SaaS). “IaaS provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer. PaaS is intended to enable developers to build their own applications on top of the platform. SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security. [3]

II- RESEARCH METHODOLOGY

As discussed earlier, we used NIST SP 8000-30 Rev1 [5] to assess the risk of the cloud computing services in India. The six-steps used in NIST SP 800-30 Rev 1 are shown in figure 1 which include Identify Threat Sources,

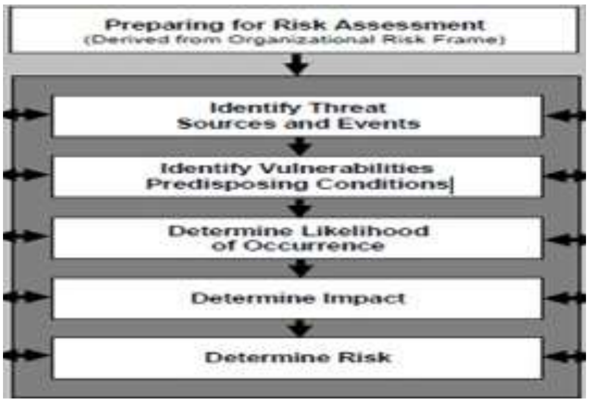

Preparing for Risk Assessment
(Derived from Organizational Risk Frame)
Identify Threat Sources and Events
Identify Vulnerabilities Predisposing Conditions
Determine Likelihood of Occurrence
Determine Impact
Determine Risk

Fig 1- NIST 800-30 Rev 1[5]

Identify Threat Events, Identify Vulnerabilities, Determine Likelihood, Determine Impact, and Determine Risk.

To provide more detail checklist in assessing each step of the framework, we used RIIOT Method [6]. Figure 2 shows five steps taken into consideration in RIIOT (Review Document, Interview Key Personnel, Inspect Security Control, Observes Personnel Behavior, and Test Security Control) Method. Finally, to cover key management aspects, i.e., cloud models and domains, of cloud security, we used CSA Guide version 2.1 which is shown in diagram part [7].

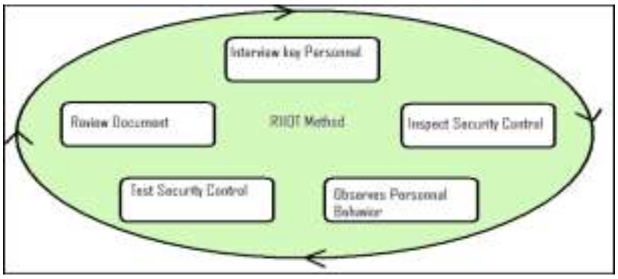
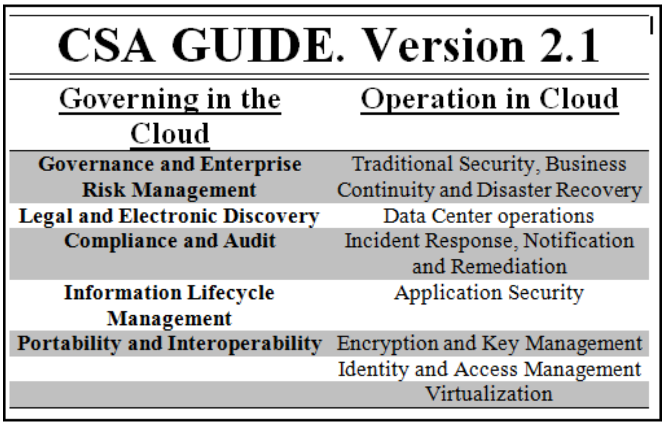


Fig 2 - RIIOT Method

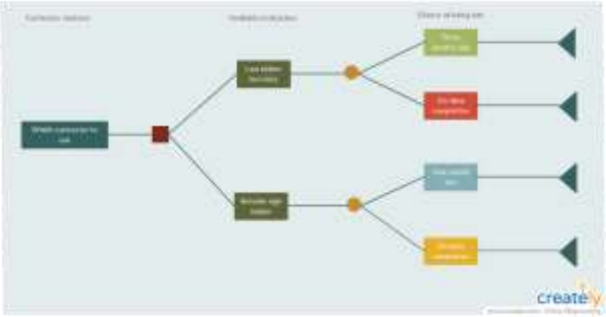
The combination of NIST 800 SP 800-30 Rev 1, RIIOT Method provides us strong foundation for calculating the risk depicting business aspects that each of the provided need to focus on in cloud computing services for general business.

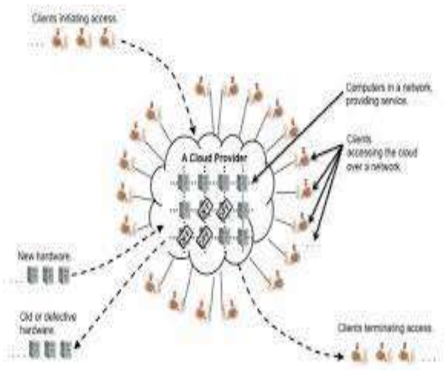
III-DESIGN



CSA GUIDE. Version 2.1

Governing in the Cloud	Operation in Cloud
Governance and Enterprise Risk Management	Traditional Security, Business Continuity and Disaster Recovery
Legal and Electronic Discovery	Data Center operations
Compliance and Audit	Incident Response, Notification and Remediation
Information Lifecycle Management	Application Security
Portability and Interoperability	Encryption and Key Management
	Identity and Access Management
	Virtualization




Clients initiating access.
Computers in a network, providing service.
A Cloud Provider
Clients accessing the cloud over a network.
New hardware.
Old or defective hardware.
Clients terminating access.

IV-CONCLUSION

Based on our research, risk of internal threats seems to be the highest risk for all risks evaluated. Internal threats include such as malicious insider, which is very hard to predict and prevent. This particular insider threat is also one of the sources for other threats, such as data loss or leakage. For external threats, all cloud providers have already applied some kind of protection and security controls to prevent possible external attacks. Nevertheless, with the help of insiders followed by ambush attack which make all protection useless.

Cloud providers in India need to focus on providing and maintaining the available and future security controls. Layered defense is one of the best ways to provide better security. On the other hand, to further reduce the risk of insider threats, complex security policy, monitoring and well employee job management are the critical factor for success.

Based on our research, local cloud providers, such as CBN,JIO,AIRTEL and TELKOM, still need to improve further their security services, especially in IaaS model (Microsoft has definitely has defined services in this model [10]). As always, continuous improvement to assess current security controls is needed to minimize security risks and prevent the possible attack

Therefore, recommendation to cloud provider is to establish their security policy on the employee movement. Malicious insider, shared technology and data loss will occur due to the growth of cloud business in India. In order to prevent those threats due to accident, security policy related employee should prioritize.

One example of such policy which requires the resigning employee is forbid from joining any companies that provide similar services for at least the next 6 months. This kind of policy has become an industry standard for banking and insurance companies. An example of such rule written on PRUDENTIAL Agency applied [11] “Telah mengakhiri hubungan dan/ atau perjanjian keagenan dengan perusahaan asuransi lain sekurang kurangnya 6 (enam) bulan.” CBN, as one of the cloud providers, has applied this policy, unfortunately other providers have not. Hence, the risks due to these threats are still quite high in the near future unless proper security policy is enforced.

For cloud customer there are several factors that need to be considered in choosing the right cloud provider. First, Service Level Agreement (SLA) is one of the most important things that customer need to focus on. The downtime should be stated clearly and well described before customer signed any SLA. SLA are crucial and the strongest written paper that can be used in the court if any agreements cannot be fulfilled by the provider [12]. Next, Datacenter specification and location is another important aspect in choosing cloud provider. In general, most people either ignore or do not clear idea about where their data is being stored, simply because customers just trust the provider they subscribed to. Finally, customers need to pay much more attention on how each of cloud providers in handling incidents and in providing services to customer when incident happened.

Based on latest RIM statement there are no datacenter in India that stand on tier 3 with specification availability 95.982%, multiple power and cooling distribution path and downtime with 1.6 hour per years [13]. With this kind of specification, India is not ready to support especially tier 3 and 4 data centers in India. This is also confirmed by Microsoft, Google and VMware [14]. Hence, recommendation for Indian government is to build a new infrastructure that are needed and establish the security law that allows large cloud providers to start providing their business in India. Another important and urgent issue how natural disaster such as flood is resolved in Jakarta. With Jakarta, as the capital of the nation where there is no clear resolution of flood is laid out by the government even with enough budget is allocated [13]. The impact of flood to data center has been experienced by TELKOM in 2007, even though no serious damage to existing infrastructure has occurred but the flood has forced TELKOM unable to provide its services for several days.

As for recommendation for future work, the largest issue is to continuously assess the vulnerability of the system through Cloud Providers Started Selling Cloud Technology in India Services CBN August 2010 (prototype) 1 October 2011 (launch) IaaS Model Telkom Years 2009(first) Year 2010 (second) First(PaaS and IaaS models) Second (SaaS model) HP Not Available IaaS, PaaS and SaaS Microsoft Year 2012(Azure) Year 2011 planning 2012 selling IaaS, PaaS and SaaS regular penetration testing and regularly evaluate effectiveness of existing security controls. More research is also needed on the threats that cover each of cloud models (IaaS, PaaS, SaaS) in more comprehensive

REFERENCES

[1] *Vivek Kundra. (2011, july) Seeking Alpha. [Online].*

[2] *Rehan Saleem, "What's New About Cloud Computing Security?" 2011.*

[3] *John Sihotang. (2011, january) Slideshare. [Online].*

[4] *Tim Mather, "Data leakage prevention and cloud computing," [Online]*

[5] *NIST Special Publications on Guide for Conducting Risk Assessment. [Online] Available:Vivek Kundra. (2011, july) Seeking Alpha. [Online].*

[6] *Rehan Saleem, "What's New About Cloud Computing Security?" 2011.*

[7] *John Sihotang. (2011, january) Slideshare. [Online].*

[8] *Tim Mather, "Data leakage prevention and cloud computing," [Online]*

[9] *NIST Special Publications on Guide for Conducting Risk Assessment. [Online]*

[10] *Prudential. [Online].*

[11] *SLA Toolkit, Service level agreement and guide.,2008.*

[12] *RIM.(2011, Dec.)Detik. [Online].http://www.detikinet.com/read/2011/12/19/105042/1794253/328/untung-rugi-data-center-blackberry-di-india*

[13] *Tifatul Sembiring, "Tahun 2012 jaringan telekomunikasi asing wajib miliki data center di India," in REPUBLIKA, Jakarta,2011.*