RISK ANALYSIS AND COMPARATIVE STUDY OF THE DIFFERENT CLOUD COMPUTING PROVIDERS IN INDONESIA

Charles Lim[1], Alex Suparman[2],

[1]*SWISS GERMAN UNIVERSITY,*

Edutown, BSD CITY, Tangerang 15339, Indonesia

[1]Charles.lim@sgu.ac.id

[2]*BINUS UNIVERSITY,*

Jakarta, INDONESIA

[2]ALEX_CH4NG@hotmail.com

Abstract— The objective of this research is to evaluate the risk of cloud computing in Indonesia. Risk assessment is conducted on the system and recommendation of control is provided to help cloud provider in Indonesia 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 Indonesian government to prepare the required infrastructure by cloud providers to run their business in Indonesia.

Keywords— Cloud computing, Cloud security, Risk assessment, Data centre.

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 $5 billion 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 (at least the provider bears a responsibility for security)." [3]

II. THEORETICAL FOUNDATION

In this section, several standard frameworks are analysed and compared to choose the most appropriate framework to be used for performing risk assessment of the cloud computing business in Indonesia. Following are the criteria for selecting the risk assessment framework:

1. Can be used for both organizations and individual users.
2. Focuses solely on the risk assessment processes to determine the level of risk.
3. Provides comprehensive and clear methodologies.

Table I below summarized the frameworks evaluated for the purpose [4].

TABLE I
FRAMEWORKS EVALUATED

Standard	**Descriptions**
ISO 13335	It concentrates on technical security controls procedures
ISO 27000	It focuses on the management aspects of security management
ISO 31000	Broad guidance on risk management
NIST SP 800-16	Focuses heavily on the control side (both operation and technical controls)
NIST SP 800-39	Similar to ISO 27001, which is focusing on management aspects of Information Security
AS 4360	It provides risk identification, analysis, estimation, evaluation, and treatment. The standard needs continuous communications with stakeholders which will be better used for business instead of individuals.
OCTAVE	It is intended to be used solely by organizations

NIST SP 800-30 Rev 1	The framework for risk assessment

NIST SP 800-30 Rev1 not only provides the most appropriate framework for risk assessment but also provide a clear step by step methodology. In addition, it also provides comprehensive figures and tables to ensure that the assessment is conducted accurately. The risk table generated from the risk assessment will be combined with the risks described in CSA guide 2.1 so that each threat can be easily identified and mapped to their relevant controls and specification from the combined table.

III. Research Methodology

As discussed earlier, we used NIST SP 800030 Rev1 [5] to assess the risk of the cloud computing services in Indonesia. The six-steps used in NIST SP 800-30 Rev 1 are shown in figure 2 which include Identify Threat Sources, Identify Threat Events, Identify Vulnerabilities, Determine Likelihood, Determine Impact, and Determine Risk.

Figure 2 NIST 800-30 Rev 1[5]

To provide more detail checklist in assessing each step of the framework, we used RIIOT Method [6]. Figure 3 shows five steps taken into consideration in RIIOT (Review Document, Interview Key Personnel, Inspect Security Control, Observes Personnel Behaviour, 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 [7].

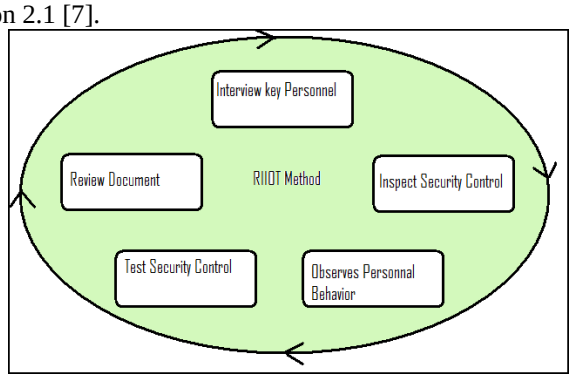

Figure 3 RIIOT Method

The combination of NIST 800 SP 800-30 Rev 1, RIIOT Method and CSA Guide ver 2.1 provides us strong foundation for calculating the risk and accurately depicting business aspects that each of the provider need to focus on in cloud computing services for general business.

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

Figure 4 CSA Guide Version 2.1[7]

CSA is the Cloud Security Alliance a group of people creating security guidance for critical areas of focus in cloud computing. The first domain in CSA guide v2.1 covers cloud architecture, while the other twelve domains are being divided into two broad categories governance and operation.

IV. Research Findings

After contacting cloud service providers in Indonesia to get some feedback how they want to be involved, 4 Internet Service Providers confirmed that they are willing to participate. There are 5 major parameters to be compared and they are: Availability, Adaptability, Data centre location, Reliable support, Security, and Multi telecommunication operator. From these items, we have found 2 major differences on the parameters, which are data centre location and multi telecommunication operator. For the datacentre location Microsoft is the only one who didn't has any datacentre running in Indonesia which is mean that customer data will be stored outside the country. For the multi telecommunication operator only CBN allows customer to choose other internet ISP as the third party for the internet services. We also performed physical inspection to the data centre when they allowed us doing so.

Eight categories of threats to cloud computing have been identified, and they are threats classification, current control, proposed control, residual risk, cloud model disturb, CSA domain and risk level result. The risk level is obtained by going through NIST 800-30 rev 1, which is based on calculated formula of likelihood and level of impact.

The table below summarized the threats, likelihood of threats, and the impact level of threats:

TABLE III
Threats, Likelihood and Impact Level

Threats	Descriptions	Likelihood	Impact
Abuse and nefarious use	Threat source of malicious user or bad user, the possible vulnerabilities for this threat are internet protocol, insufficient	L	L

	network based control in virtualized network.		
Malicious Insiders	Threat source of insider privileged user or administrator. The possible vulnerabilities for this threat are insecure cryptography, managerial security, and background check and security policy.	L	M
Shared technology issues	Threat source of insider privileged user or administrator and accidental ordinary user. The possible vulnerabilities for this threat are job distribution, physical security, identification cards, guards, electronic monitoring vulnerabilities.	L	H
Data Loss	The threat source of insider and outsider. The possible vulnerabilities for this threat are data recovery, technical security, insecure cryptography, firewall, IDPS and antivirus vulnerabilities.	L	VH
Natural Disaster	Natural disaster (see notes below)	L	L

L=Low; M=Moderate; H=High; VH=Very High

Note on the natural disaster threats, we have limited the scope of threats to floods, earthquake, fire and hurricane as the possible threat sources. Hence, the risk level for most of the threats above is low, except on the data loss issue, with the risk level of moderate.

The combination table between NIST 800-30 rev 1 and CSA guide version 2.1 has eight category which are Threats, Threats classification, current control, proposed control, residual risk, model disturb, CSA domain and risk level. Based on this combination table it is easier to understand the condition of each threats how to handle using the given control and which area did the threats disturb.

TABLE IIIII
COMBINED TABLE USING NIST AND CSA PARAMETERS

Threats	Threat Classification	Proposed Control	Cloud Models	Risk Level
Abuse and nefarious use	External Threats	Layered Encryption	IaaS & Paas; Domain 8 & 9	L
Malicious insider	Internal Threats	Advanced Security Policy, Layered Encryption, Job Specification, and comfortable working environment	All Models; Domain 2 and 7	M
Shared technology issues		Advance Security Policy, law, job specification and maintain working environment.	IaaS, Domain 8 & 13	L
Data Loss	Internal & External Threats	Advance security policy, law, job specification, maintain comfortable work environment, advance cryptography and background check	All models; Domain 5, 11 and 12	M
Natural Disaster	Natural	Disaster Recovery Plan	All Models; Domain 2, 7, 8 & 12	L

L=Low; M=Moderate; H=High; VH=Very High

Note residual risks for data loss are device loss or key of encryption loss, admin side, and malicious insider hard to detect, economic problem and law.

The above table shows risks with several controls being proposed or applied, the internal threats can be classified as dangerous with two moderate risk level. As for the external threat, the number of control provided by the cloud providers such as firewall and Incident response team are sufficient enough to protect the system from the external attack. This make the risk rating is only low.

The limitation of this research project is that the scope is limited to cloud computing services provided in Indonesia. Since cloud computing service is an emerging service in Indonesia (please see table IV below), this in turn makes the

research much more challenging to find resources for this study. In addition, some statistics for threats likelihood can't be obtained since they just started their businesses. Furthermore two processes in the RIIOT method cannot be completed due to the company regulations which prevent penetration testing to their system and limited time available. All cloud providers put the restrictions on doing penetration testing, which usually include vulnerability scanning and the control testing [6]. For this reason, these two processes will be added as the recommendation for future research.

TABLE IVV
CLOUD SERVICE AVAILABILITY

Cloud Providers	Started Selling Cloud Technology in Indonesia	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

V. CONCLUSIONS

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 Indonesia 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 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.

VI. RECOMMENDATION

In this section, we provide recommendation for cloud providers, cloud customers, Indonesian government and future research works respectively.

Several experts predicted that in years 2016 almost all company in Indonesia will move their system to cloud, mostly likely of private, public or even hybrid cloud models. 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 Indonesia. In order to prevent those threats due to accident, security policy related employee should prioritized. 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 provider, 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 at DetikInet, there are no datacenter in Indonesia that stand on tier 3 with specification availability 99.982%, multiple power and cooling distribution path and downtime with 1.6 hour per years [13]. With this kind of specification, Indonesia is not ready to support especially tier 3 and 4 data center in Indonesia. This is also confirmed by Microsoft, Google and VMware [14]. Hence, recommendation for Indonesian 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 Indonesia.

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

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]. Available: http://seekingalpha.com/article/283444-cutting-government-spending-with-cloud-computing

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

[3] John Sihotang. (2011, january) Slideshare. [Online]. Available: http://www.slideshare.net/jhotank62/cloud-computing-fundamental

[4] Tim Mather, "Data leakage prevention and cloud computing," [Online] http://www.kpmg.com/Globa1/Pages/default.aspx

[5] NIST Special Publications on Guide for Conducting Risk Assessment. [Online] Available: http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

[6] Douglas J Landoll, The Security risk Assesment Handbook. Boca Raton: Taylor & Francis Group, 2006.

[7] Cloud Security Alliance, Security guidance for cloud computing. United States: Cloud Security Alliance Guidance, 2009.

[8] Cloud Security Alliance, "CSAthreats v 1.0," ten threats cloud computing, pp. 6-14, 2010.

[9] *Cloud Computing Alliance, "CSA guid Version 1.0," Top Threats to Cloud computing, march 2010.*

[10] Microsoft Cloud. The Most Comprehensive Solution for cloud. [Online]. Availabe: http://www.microsoft.com/en-us/cloud/default.aspx?fbid=sxY8EcY_e_C

[11] Prudential. [Online]. Available: http://www.prudential.co.id/pruweb/?mn=career&smn=employees

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

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

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