Implementation of COSO ERM as Security Control Framework in Cloud Service Provider

Jarot S. Suroso
Master in Information Systems Management Bina Nusantara University,
Jln. Kebon Jeruk Raya No. 27 Jakarta, Indonesia
Email: jsembodo@binus.edu

Harisno and Johan Noerdianto
Master in Information Systems Management Bina Nusantara University,
Jln. Kebon Jeruk Raya No. 27 Jakarta, Indonesia
Email: harisno@binus.edu; jnoerd@gmail.com

***Abstract*—Computing technology has been evolution to cloud technology nowadays. Cloud computing has scalability on providing network access to a shared pool computing resources and applications with quick provisioning process and minimum effort. A Cloud service provider (CSP) is a third-party vendor that provides application delivery, hosting, monitoring, and other services through cloud computing (Horwath, 2012). Cloud service in an IT function still requires standard and frameworks. Company PT. Media Andalan Bersama, as a CSP, needs to understand the standards and frameworks that obtain IT governance in a cloud environment. There are some challenges in cloud computing regarding privacy, confidentiality and security of data and threat to business continuity. Several popular IT Governance and Standards Frameworks are COSO, COBIT, ITIL, and ISO 27001/9000. Applying COSO ERM framework to the business processes in cloud providers provide comprehensive view of risks, benefits and action plan options.**

***Index Terms*—cloud computing, risk management; COSO ERM, cloud service provider**

I. Introduction

Cloud services in the functioning of the Information Technology (IT) still requires standards and frameworks. PT. Media Andalan Bersama (PT. MAB) with its brand products "d'awan" as a Cloud Service Provider (CSP) needs to understand the standards and frameworks to obtain Information Technology (IT) governance in a cloud environment.

Security in cloud computing is one of the major risks that must be managed by the CSP. Compliance with security standards, the target of cyber-attacks, data and information leakage in the cloud environment are some security risks that must be anticipated by the CSP. Ref. [1] had discussed COSO ERM to mitigate cloud business challenges. Ref. [2] had discussed this issue in brief related to a risk and control framework for cloud computing and virtualization. Handling the security aspects related to the use of IT is required by the control standards and well documented by adopting COSO ERM framework.

Policy and decision making based on of the board of directors decision, is not yet available for the overall standards and well documented business processes. So it is necessary to study the compliance management of PT. MAB against COSO ERM framework.

The COSO ERM framework will be used for identification of risks and mitigation strategies within cloud computing in PT. MAB. Thus executives of PT. MAB will be able to identify, monitor, and mitigate or accept the risks that come with using cloud computing. COSO ERM framework will assist management of PT. MAB to implement risk management and weigh the risks in taking operational decisions related to cloud computing technology, and provide standard security controls that can be applied in the course of business processes and IT infrastructure of PT. MAB.

II. Method

The research method that has been used as follows:

1) Literature review (Library Research)

Studies conducted by collecting articles on the internet and other written sources to obtain theories and scientific knowledge and opinions of certain parties to support the process of research is being done.

2) Field Study (Field Research)

Field Study conducted with following methods:

- Interviews and questionnaires with the directors or the management of PT. MAB.
- Direct observation to the object of study and examination of related documents.

3) Research Parameter

The parameters used in this research is the COSO ERM framework. Risk assessment method selected by author to analyze the risk in this research is a qualitative method, as indicated in Fig. 1.

Manuscript received January 10th, 2017; revised March 8th, 2017.

doi: 10.18178/joams.5.4.322-326

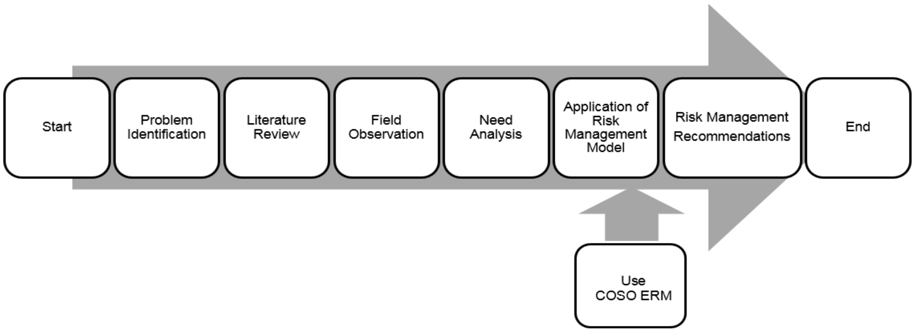
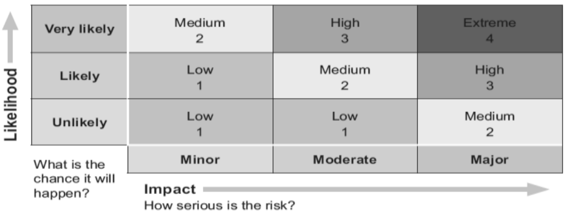


Figure 1. Research framework

In order for the COSO ERM framework to be implemented effectively, risk assessment criteria must be developed before the risk assessment process starts. The same common criteria must be used by all business units, corporate functions and large capital projects. Using the same scale across all business units helps to ensure consistency within the process. The scales should have the right balance between simplicity and precision. The staff members using the scales should be able to assess risks without wasting time on immaterial decisions. All of the risk events that are identified are supposed to be assessed using the same impact and likelihood scales.

Risks are analyzed based on the likelihood and impact and the subsequent results of risk analysis served as the basis for determining how risks should be managed. The risk assessment can be viewed from two perspectives: the likelihood (possibility) and impact, as indicated in Fig. 2.


Likelihood
What is the chance it will happen?
Impact
How serious is the risk?

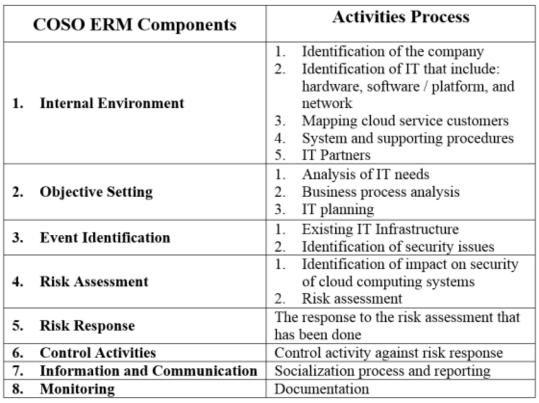
Very likely	Medium 2	High 3	Extreme 4
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
	Minor	Moderate	Major

Figure 2. Likelihood and Impact Matrix [8]

III. Result and Dicussion

COSO ERM framework has eight major components and can be mapped to processes in research activities as follows, as indicated in Table I.

TABLE I. COSO ERM Implementation In PT. MAB



COSO ERM Components	Activities Process
1. Internal Environment	1. Identification of the company 2. Identification of IT that include: hardware, software / platform, and network 3. Mapping cloud service customers 4. System and supporting procedures 5. IT Partners
2. Objective Setting	1. Analysis of IT needs 2. Business process analysis 3. IT planning
3. Event Identification	1. Existing IT Infrastructure 2. Identification of security issues
4. Risk Assessment	1. Identification of impact on security of cloud computing systems 2. Risk assessment
5. Risk Response	The response to the risk assessment that has been done
6. Control Activities	Control activity against risk response
7. Information and Communication	Socialization process and reporting
8. Monitoring	Documentation

A. *Internal Environment*

PT. MAB is a provider of streaming video content delivery solutions by implementing a cloud computing-based technologies. The services offered include Streaming CDN Acceleration, CDN Web Acceleration, Maya Media Management, as well as secure load balancer, compute and storage for cloud services (cloud service). Currently PT.MAB already has two datacenters in the area of Jakarta city that was built since the beginning of 2014 and is supported by high-tech infrastructure. Infrastructure owned by PT. MAB is composed of several elements according to function either hardware or software, namely: network router and switch fabric, firewall, load balancer, server, storage, cloud system, the operating system (OS), and video compression.

PT. MAB provides a Content Delivery Network (CDN) by adopting cloud technology and VCMS. Cloud architecture PT. MAB consist of components: front-end platform (client and mobile devices), back-end platform (server, storage), cloud-based delivery, and network (Internet, intranet, inter-cloud). Management cloud (cloud management) PT. MAB consist of software and technology used to help ensure that resources based on cloud computing work optimally and properly interact with the user and other services.

VCMS technology forms the core of the solutions and services provided by PT. MAB which serves to organize and orchestration of system ingest, transcoding, encryption, and content delivery to the origin server. VCMS in the Web Content Management Service has function for the editors so they can control and do manipulation of content loaded. The system is also designed to enable Over-The-Top (OTT) service platform based cloud as a wholesale solution for operators to broadcast multi-screen social video and monetization. OTT Platform system combines online, mobile, social and video delivery so that providers can broadcast video content seamlessly into the audience, engage audiences on any screen, as well as premium content monetization.

To improve the security system in the CDN infrastructure, PT. MAB implements firewall device in existing networks on each datacenter. Firewalls monitor and filter data traffic heading out of the network or CDN. To take control of users accessing content CDN, PT.

MAB implements user management system with methods Single-Sign-On (SSO) and digital rights management.

B. Objective Setting

COSO ERM framework provides references with respect to the use of cloud technology computing in the cloud services offered by PT. MAB:

1) Determination of business processes

PT. MAB has set the business process or Standard Operation Procedure (SOP) as a reference in the company's business activities, as indicated in Table II.

TABLE II. BUSINESS PROCESS SUMMARY

No	Business Process	Business Activities
1	Business Process Sales Order	Marketing and sales
2	Business Process Live Streaming Implementation	Service implementation
3	Business Process Maya VCMS	Service implementation
4	Business Process Application Development	Application development
5	Business Process Custom Application Development	Application development
6	Business Process Approved Application	Application development
7	Business Process virtual server cloud	Service implementation
8	Business Process problem handling	Operational
9	Business Process Monitoring Preventive	Operational

2) Determination of cloud computing implementation model

In the early stages of design and design of cloud computing systems PT. MAB implementing public cloud models where cloud computing services and existing CDN network can be accessed from the Internet. Along with business development, cloud computing security considerations as well as the needs of customers who require their private cloud, then the current PT. MAB implement a hybrid cloud models, a combination of public cloud and private cloud so that services can be tailored to customer requirements.

3) Determination of the cloud computing service model

PT. MAB provides all three types of cloud computing services model SaaS, PaaS and IaaS to meet customer requirements.

4) Determining the risk appetite of the company

Selection of risk response is done by comparing the results of risk analysis with risk appetite. Management PT.MAB choose four alternative risk response: avoidance, acceptance, reduction), and sharing the risk.

C. Event Identification

Risk identification is required to determine the risks that may occur, causing potential losses and the impact that may result. The process of identifying the incidence and risk factors was conducted using questionnaires or interviews and reviewing some previous research related to the risks that may occur in the use of cloud computing technologies with focus on security and operational control of the cloud computing infrastructure and CDN PT. MAB.

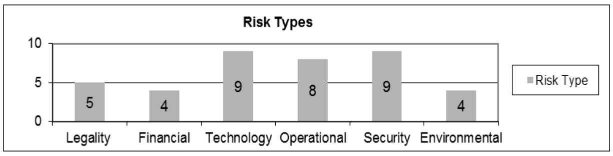


Figure 3. Risks Types

The composition of the number of types of risks from the observation in PT. MAB are risk in security and the technological aspects of each of 9 risks, operational aspects 8 risks, legal aspects 5 risks, and financial and environment aspects respectively of 4 risks (Fig.3).

D. Risk Assessment

Based on the identified risks, data processing and assessment is necessary to determine the profile of each risk. With the risk assessment, it can be known the level of impact and likelihood so the mapping risks based on priority level, which is very high (extreme), high, intermediate (medium) or low. The risk assessment can be viewed from two perspectives: the likelihood (possibility) and impact. The higher the degree of impact and likelihood of the higher overall. Furthermore, from these two measures can be known matrix of both dimensions. Percentage matrix greatest risk level per level at low risk by 38%, moderate risk (medium) by 36%, high risk by 18% and very high risk (extreme) by 8%, as indicated in Fig.4.

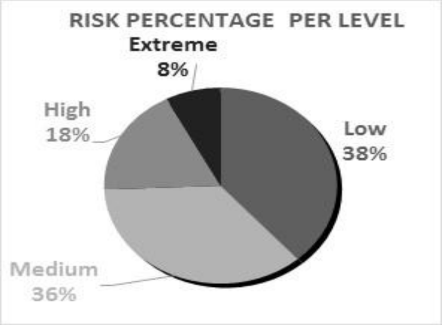


Figure 4. Risk Percentage per Level

Identified very high level (extreme) risks are as follows:

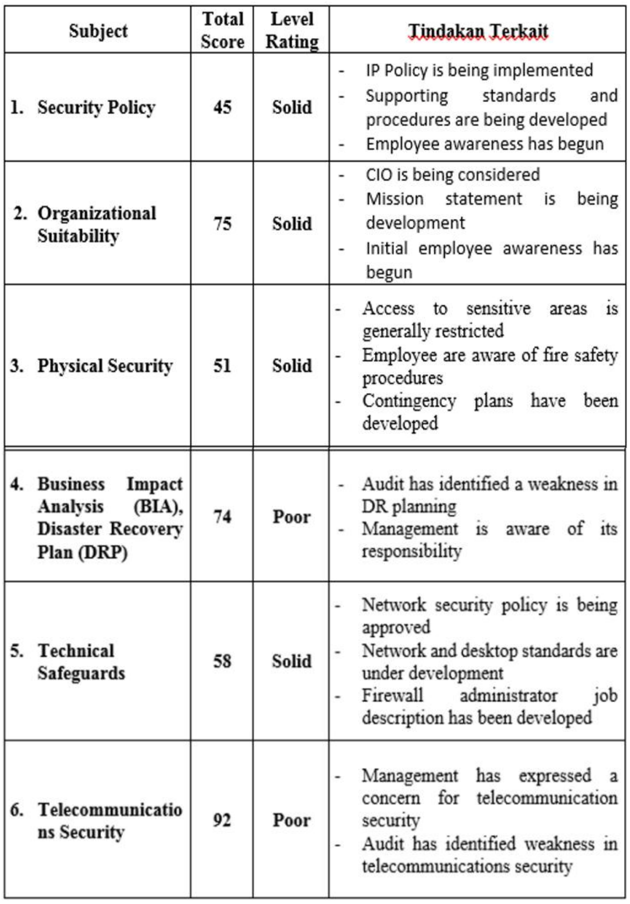
a) Aspects of the technology: The availability of experts in the field of information systems security.

b) Aspects of the technology: power supply has sufficient capacity and has a backup system.

c) Security aspect: The risk of cyber-crime such as hackers, phishing, scamming, and a Distributed Denial-of-Service (DDOS).

In conducting research and field studies, interviews with questionnaires have been conducted also with the directors or the management of PT. MAB. The questionnaire comprised of 6 important subjects and every question has given ratings. Furthermore, all values for each of the subjects is summed so it can be a range of values, the level of assessment and action-related activities and in accordance with Table 1. below. The use of the questionnaire aims to identify and analyze the risks of information security and information protection (IP) program in a company [8].

TABLE III. RESULTS OF THE ASSESSMENT QUESTIONNAIRE



Subject	Total Score	Level Rating	Tindakan Terkait
1. Security Policy	45	Solid	- IP Policy is being implemented - Supporting standards and procedures are being developed - Employee awareness has begun
2. Organizational Suitability	75	Solid	- CIO is being considered - Mission statement is being development - Initial employee awareness has begun
3. Physical Security	51	Solid	- Access to sensitive areas is generally restricted - Employee are aware of fire safety procedures - Contingency plans have been developed
4. Business Impact Analysis (BIA), Disaster Recovery Plan (DRP)	74	Poor	- Audit has identified a weakness in DR planning - Management is aware of its responsibility
5. Technical Safeguards	58	Solid	- Network security policy is being approved - Network and desktop standards are under development - Firewall administrator job description has been developed
6. Telecommunications Security	92	Poor	- Management has expressed a concern for telecommunication security - Audit has identified weakness in telecommunications security

Based on above results of risk assessment of information security can be identified that there are two (2) subjects important that they have a low level rating (poor), the Business Impact Analysis (BIA), Disaster Recovery Plan (DRP), and Telecommunications Security. Factors that affect the low level of information security risks in the field of BIA and DRP include:

a) The absence of DRP coordinator in the company and the definition of duties and responsibilities.
b) The backup datacenter location is near to the primary datacenter.
c) The absence of an automatic system restart procedure and recovery to restore data files in the event of failure of data processing.
d) Unavailability of contingency plans hardware, software, communications software, and staff.
e) Lack of training conducted for all relevant personnel on backup procedures, recovery and contingency operations.
f) DRP test activity has never been done.

E. Risk Response

Based on the results of previous risk assessment can be used as a reference to determine appropriate risk response. The management of PT. MAB do four alternative risk responses: avoidance, acceptance, reduction, and share the risk (sharing).

a) Accept the risk: PT. MAB choose response to the risk of receiving these risks when it comes to legality. As one of the CSP in Indonesia, PT. MAB has to comply with laws and regulations that apply in the country of Indonesia. PT. MAB has hold official permission from the government in terms of the company license, CSP business license, and a broadcasting license content in the cloud computing system and CDN. In addition to the risks associated with service features such as system for video compression, 24x7 support for customers, guarantees data security for customers, and the support system monitoring devices, as well as supporting facilities datacenter as the availability of datacenter cooling systems, adequate fire extinguishing systems, CCTV surveillance cameras, temperature and humidity monitoring devices, then PT. MAB will tend to accept those risks. Risks caused by natural disasters such as earthquakes and floods constitute force majeure conditions and beyond the company's ability to avoid the PT. MAB also accepts the risk.
b) Avoid the risk: PT. MAB choose risk response to avoid these risks if the risk can cause harm and disruption of services such as cloud computing and CDN configuration error (human error) and access to the device from unauthorized parties.
c) Sharing the risk: PT. MAB choose risk response by dividing the risk if these risks can be mitigated through cooperation with other companies such as payment gateway and experts in the field of information systems security by outsourcing.
d) Reducing the risk: PT. MAB choose risk response by reducing the risk if the risk can be mitigated by preventive measures so that the impact of these risks can be reduced such as:
    - Equipment maintenance and regular checks of the building structure.
    - Testing backup power supply systems such as UPS and generators) periodically.
    - The use of security systems such as firewalls and antivirus software.
    - The use of telecommunications network with a backup system and the different lines and Internet connections with different ISP.
    - Training of cloud computing and CDN technology to the appropriate technician expertise.
    - The use of the access control system or device to access the database remotely.

F. Control Activities

The next step is risk control activities which this step is necessary to ensure the selection of risk response by PT. MAB can be implemented properly. Variety of risk control activities both preventive and corrective are required.

G. Information and Communication

To communicate above results of the analysis of risk management information effectively, then PT. MAB requires techniques that facilitate communication so that information can be received and followed up by the management and the units that has responsible for sales and marketing activities and operations of the company. The information is needed at all levels of an organization to identify, assess and respond to risks. Some models of communication adopted by the PT. MAB for the dissemination and reporting of risk management analysis are as follows:

a) Monthly meetings of directors and top management of the company regularly.
b) Weekly meeting of the operational activities.
c) Weekly meeting on marketing activities.
d) Daily communication using email.

H. Monitoring

The entire risk management activities need to be monitored and evaluated by PT. MAB through ongoing management activities or separate evaluations including evaluations of activities of daily information on running business and operational activities of the company. PT. MAB conducting separate evaluation of change control in the cloud computing infrastructure and CDN with the involvement of external consultants. In evaluating the risk management company, PT. MAB reviewing or developing documentation processes and other activities to facilitate the evaluation team to understand units, processes, or risk and response. Documentation considered in the evaluation includes:

a) The organizational structure and the job description.
b) Standard Operation Procedure (SOP)
c) Business Process
d) Key Performance Indicators (KPI)

IV. Conclusions

1. Application of COSO ERM framework model is in accordance with the conditions of PT. MAB as risk management tool related to the use of cloud computing technology. The management of PT. MAB has conducted an objective setting by defining business processes, the implementation model and the model of cloud computing services as well as the risk appetite to pick alternative risk responses.
2. Application of COSO ERM framework model can be used to assess 39 risks based on observations and interviews with PT. MAB and the assessment results of some previous research and models related to cloud computing risk management framework that has been provided. These risks can be grouped into the legal aspects, financial aspects, technological aspects, operational aspects, security aspects and environmental aspects.
3. Based on the survey results revealed that the risk level is very high (extreme) covers the technological aspects, namely the availability of experts in the field of information systems security and adequate power supply capacity and power backup system, whereas in the security aspect is the risk of cyber-crime such as hackers, phishing, scamming, and a Distributed Denial-of-Service (DDOS).
4. Based on the results of questionnaires and interviews regarding risk management, information security and Information Protection (IP) program in PT. MAB that of the six subjects that are PT. MAB has level rating of "solid" in terms of Security Policy, Organizational Suitability, Physical Security, Technical Safeguards, and it has level rating of "poor" in terms of the Business Impact Analysis (BIA), Disaster Recovery Plan (DRP) and Telecommunications Security.

References

[1] K. Almgren, “Implementing COSO ERM framework to mitigate cloud computing business challenges,” *Int. J. Bus. Soc. Sci.*, vol. 5, no. 9, pp. 71–76, 2014.

[2] M. Carroll, P. Kotze, and A. der Merwe, “A risk and control framework for cloud computing and virtualisation: enabling technologies,” *CSIR Sci. Scope*, vol. 6, no. 2, pp. 62–63, 2012.

[3] C. Horwath, W. Chan, E. Leung, and H. Pili, “Enterprise risk management for cloud computing,” *Comm. Spons. Organ. Treadw. Comm.*, pp. 4, 2012.

[4] R. Moeller, *COSO ENTERPRISE RISK MANAGEMENT UNDERSTANDING THE NEW INTEGRATED ERM FRAMEWORK*. New Jersey: John Wiley & Sons, Inc., 2007.

[5] E. L. Carroll, “Occupational fraud : A survey,” *A thesis Submitt. to Fac. Univ. Mississippi Partial fulfillment Requir. Sally McDonnell Barksdale Honor. Coll.*, no. May, 2015.

[6] Z. Enslin, “Cloud computing : COBIT-mapped benefits , risks and controls for consumer enterprises,” *Thesis Present. Partial fulfilment Requir. degree Masters Commer. (Computer Audit. Stellenbosch Univ.*, no. March, 2012.

[7] R. R. Moeller, *COSO Enterprise Risk Management Establishing Effective Governance, Risk, and Compliance Processes*, 2nd ed. New Jersey: John Wiley & Sons, Inc., 2011.

[8] T. R. Peltier, *Information Security Risk Analysis*, 3rd ed. New York: CRC Press, 2010.

Jarot S. Suroso, Associate Professor in Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia. Doctor of education from Jakarta State University, Indonesia and also Doctoral Sandwich of Competitive Intelligence from Aix Marseille University France. He is graduated from master degree of Ecole Superiere d’Ingenieur de Marseille France.

His major research interests include management information system, competitive intelligence, knowledge management, computer network, e-learning, multimedia and research methodology. He can be reached at jsembodo@binus.edu.

Harisno, Associate Professor in Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia. Doctor of education from Jakarta State University, Indonesia.

His major research interests include Knowledge Management System; IS Strategic Plannng; Decision Support System; E- Lesarning; IT Scorecard; Business Process Management. He can be reached at harisno@binus.edu.

Johan Noerdianto, Student in Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia. His major research interests include Security Control Framework, Cloud Service etc. He can be reached at jnoerd@gmail.com.