Assessment of ISMS Based On Standard ISO/IEC 27001:2013 at DISKOMINFO Depok City

Nurbojatmiko,
Information System of Scince and Technology Faculty,
UIN Syarif Hidayatullah Jakarta
nurbojatmiko@uinjkt.ac.id,
Aries Susanto,
Information System of Scince and Technology Faculty,
UIN Syarif Hidayatullah Jakarta
aries.susanto@uinjkt.ac.id,
Euis Shobariah.
Information System of Scince and Technology Faculty,
UIN Syarif Hidayatullah Jakarta
euissh23@gmail.com

Abstract: This research is done on the Data and Information Division at the Department of Communications and Information Technology at Depok City (DISKOMINFO Depok City). The problems that occur are no frameworks and guidelines for information security. The handling of information security issues are still dealt with in accordance with the requirements and in accordance with the knowledge of employees. ISMS planning methods using PDCA (Plan- Do- Check -Act) in accordance with the standard ISO 27001 : 2013 . It is necessary for an assessment of the Information Security Management System (ISMS).

Keyword: ISO 27001:2013, Information Security Management System, ISMS, Assessment, Plan Do Check Act, PDCA

I. INTRODUCTION

Information security management is important for Data and Information Division at the DISKOMINFO Depok City Government, because it has the duty to organize activities in the field of communication and information technology to assist in the governance of Information and Communication Technology in Depok City. In addition DISKOMINFO Depok City has a role to fulfill the need for information with the development of information technology and services for data processing.

As government agencies have a role to data and information management, governance should have good information security governance. But the reality has not had guidelines related to information security process. It was caused by a lack of understanding about the risk of information loss and information security controls. DISKOMINFO Depok City has never perform an audit of information technology governance, to be able to assess the extent to which the organization is run for the benefit of society, particularly in the field of information technology.

In journal, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Control", explores the role of information security within COBIT and describes mapping approach of COBIT processes to ISO/IEC27001 controls for information security management [5]. And "Cost-Benefit Trade-Off Analysis of an ISMS based on 27001", this papers propose using combinatorial optimization. Such optimization should weigh the benefit of a policy in term of avoiding, mitigating or transferring the risk up to some predetermined investment limit [6]. On paper "Information Security Management System Standards: A Comparative Study of the Big Five", introduce various information security standards briefly and then provide a comparative study for major information security standards, namely ISO27001, BS 7799, PCIDSS, ITIL and COBIT. And also provide a picture of the position and specialization of each standard,

adoption by countries and their usability levels [7].

This Research on information security management system as a first step to secure the information by identifying assets, provides a description of the risk occurring, the impact and control of information security risks. Phase control of information security risks in the form of objective election on information security controls.

The method of collecting data through observation, questionnaires, literature and interviews. The results of this research are expected to recommendations of security controls that can be used as guidelines and procedures for the implementation of information security so as to improve information security.

II. STUDY LITERATURE

A. Information security

Information security is keeping information from the threat of fear or prove possible to guarantee and ensure business continuity, minimize business risk and maximize or accelerate decision investment and the business opportunities [1].

B. Information Security Management System (ISMS)

ISO defines ISMS to be part of the overall management system , to establish, implement , operate, monitor , review, and improve information security . ISMS is a process created by business risk approach to plan (plan) , operates and implements (do) , review and monitor (check) and to improve and maintain or develop the (act) to the organization's information security [2].

C. ISO 27001

ISO 27001 provides guidelines for implementing ISMS, and to obtain international certificates from a third party . It was to prove that the security controls exist and operate in accordance with the requirements of the standard. ISO 27001 ISMS describes the system as the overall management of business risk approach that aims to establish, implement, operate, monitor, and maintain ISMS [2]

ISO/IEC 27001 : 2013, domain requirements and security controls . Security controls have 14 security control clauses, 35 Control Objectives and Controls have 114 [3]. Phases of ISMS in accordance with the requirements set ISO / IEC 27001 is as [1], STAGE 1, Determine the scope of the ISMS,STAGE 2: Determining the ISMS policy, STAGE 3: Determine how the risk assessment, STAGE 4: Identification of risk, STAGE 5: Analysis and evaluation of risk, STAGE 6: Identification and evaluation of risk management election, STAGE 7 : Choosing objective control and information security controls

D. Methodology PDCA (*Plan – Do – Check – Act*)

The process approach defined in ISO/IEC 27001 in building ISMS adopt PDCA cycle (Plan - Do - Check - Act). Explanation of the PDCA model applied to ISMS processes will be presented; Plan, this phase is planning and design of the ISMS. *Do,* activity in this phase is the implementation and operation of the policy, controls, processes and procedures of the ISMS refer to stage plan. *Check,* This section discusses the activities of monitoring the implementation of the ISMS, including an evaluation and audit. *Act,* is the improvement that the repair and development of ISMS[1]

E. SSE-CMM

System Security Engineering Capability Maturity Model (SSE-CMM) describe the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. This model also highlights the relationship between security techniques and systems engineering [4].

Level Capability SSE-CMM [4], Level 1 *Performed Informally,* Level 2 *Planned and Tracked,* Level 3 *Well Defined,* Level 4 Q*uantitatively Controlled,* Level 5 *Continuity Improving.*

III. ISMS ASSESSMENT AT DISKOMINFO DEPOK CITY

A. Phase PLAN

Determining the Scope ISMS; ISMS processes and assessment activities focused on controlling

information as an asset that must be protected to the maximum. The scope includes the database, application, hardware, environmental and human resources. **Determining The ISMS Policy**; Things to consider in determining the ISMS policy at table 1, which describes the assets owned in DISKOMINFO Depok City. It's have "Dinas OPD Depok" Database Monitoring System and *Database* Budget Transparency Information System.

Table 1
Example Identify Assets

No	Name Assets	Type	Explanation	location
1	"Dinas OPD Depok" *Database* Monitoring System	Information	The database contains data Applications Monitoring System	DISKOMINFO Depok
2	*Database* Budget Transparency Information System	Information	The database contains data on Information Budget Transparency Information Application	DISKOMINFO Depok

- The scope of ISMS with the characteristics of the business, company organization, location, assets and technology companies.
- The risk management methods used in the preparation and implementation of the ISMS should be aligned with the risk management methods used by the company.
- ISMS policy document should be approved by the head of the company.

Identifying Assets and Assets Appraisal; The first step in identifying risk is to identify the existing assets in the field of Data and Information DISKOMINFO Depok associated with inforrmasi.

B. Phase DO

Identifying Assets and Assets Appraisal;

Table 2
Value of Assets

	Name Assets	Value Confidentiality (VC)	Value *Integrity* (VI)	Value Availability (VA)	Value Assets
	Database Monitoring System	3	4	4	**11**

The first step in identifying risk is to identify the existing assets in Department DISKOMINFO Depok City.

Identifying Threats and Weaknesses, Threats Calculating Value; Next will be identified weaknesses and threats on the assets of Department of DISKOMINFO Depok City. Based on ISO 27001, the input of the identification of weaknesses and threats are on the first assessment report and the results of the audit.

Table 3
Example Identifying and Assessing Threats and Weaknesses Threats

No	Incident	Type	Probabilitas	Rerata Probabilitas
1	*Hardware Failure*	Vulnerable	Medium	0.5
2	Surrounding environment	Threat	Medium	0.4
Number of Events 2		Average Number Prob.		0.9
Value threat = Average Number Prob. / Total Events				**0.45**

Analyzing Business Impact; Business impact analysis is to determine how much influence or impact of the risks posed by weaknesses and threats on the course of business processes within the organization.

Table 4
Example of Value Business Impact

No	Name Assets	Value Assets	Threat Value	BIA	Risk Value	Risk Level
1	*Database* Monitoring System	11	0.35	29.70	114.34	*High Risk*
2	*Database* Budget Transparency Information System	11	0.35	29.70	114.34	*High Risk*

phase value on the business impact of Data and Information DISKOMINFO Depok. The next

stage of assessing the risk of the author conducted on the Field Data and Information DISKOMINFO Depok. This phase aims to determine the risk that occurs directly received by the Field Data and Information DISKOMINFO Depok or still need to risk management based on risk acceptance criteria.

Table 5 Examples of Value Risk

No	Name Assets	Value BIA	Threat probability	Business Impact
1	*Database* Monitoring Sistem	99	0.3	29.70
2	*Database* Budget Transparency Information System	99	0.3	29.70

C. Phase Check

Choose Objective Control and Information Security Controls; Having measured the magnitude of the risk to the security of the information assets of Data and Information DISKOMINFO Depok, takes an action or control can reduce the risk. Selection of control and security control objective in this study is based on an objective control and control of the ISO 27001: 2013, by adjusting the results of the risk assessment on the information security assets of Data and Information DISKOMINFO Depok.

Table 6
Mapping Clause ISO 27001: 2013

Material	Clauses
Security Human Resources	7
Asset Management	8
access control	9
Physical and Environmental Security	11
security Operations	12
Management Information Security Incident	16

Determination of Value Level Using the SSE-2. CMM Maturity; The determination of the level of maturity can describe the measurement of the extent to which the Field Data and Information DISKOMINFO Depok able to meet the standards of information security management processes properly. Maturity level assessment performed on each control in accordance with the results of audits conducted.

In this study, a list of statements made on the basis of any objective security controls selected control to be applied in the field of Data and Information DISKOMINFO Depok. List this statement was made and customized based on the standard ISO 27002: 2013.

Examples of value calculation framework maturity level can be seen in Table 7, for example the calculation results can be seen in Table 8 and sample representation of the results in a radar diagram is shown in Figure 1

Table 7
Example Calculation Framework Maturity Level

8.1.2	**Asset Ownership**							
No	**Statement**	**grade**	**1**	**2**	**3**	**4**	**5**	**Value**
1	Ownership of assets must be given when the assets obtained or received by the organization	1			√			3
2	Assets are defined and reviewed periodically by the access control policies that apply.	1		√				2
3	Their proper handling when the asset for removed.	1		√				2
	Total Grade	**3**	**level of proficiency**					**2.33**

Table 8
Example Results Maturity Level Clause 8

Clause	Objective Control	Security Control	Ability Levels	Average / Objective Control
8. Asset Management	8.1 Responsibility To Asset	8.1.1 Assets Inventory	2.00	2.16
		8.1.2 Assets Ownership	2.33	
	8.2 Information Classification	8.2.1 Information Classification	1.00	1.00
		Maturity Level Clause 8		**1.58**

D. Phase Act

1. Recommendation

After conducting an objective assessment on the maturity level of control and security control information of Department DISKOMINFO Depok City subsequent recommendations that are used as suggestions for improvement of security controls. Recommendations derived from observation, interviews and questionnaires conducted by the authors.

After the entire assessment is completed next maturity level values obtained maturity level of the average of all values clause, the following is the result of maturity level of the overall average value of the clause.

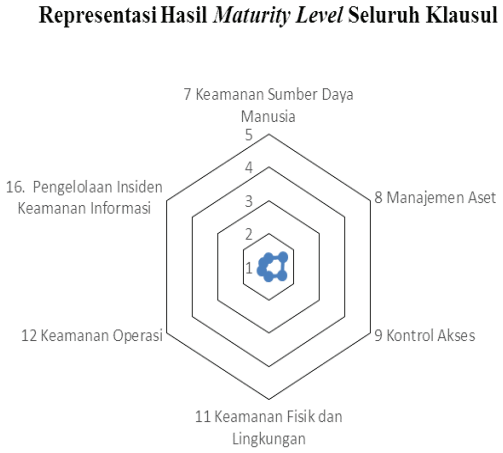

Figure 1 Representation Maturity Level Results All Clause

On figure 1, All clause of ISO 27001:2013; 8 Assets Management, 9 Access Control, 11 Physics and Environment Security, 12 Operational Security, 16 Information Security Incident Management have to representation of maturity level that point 1 until 5.

Preparation of Findings

Table 9
Results Maturity Level All Clauses

Clouse		Level Maturity
7	HRM Performance	1.25
8	Assets Management	1.58
9	Access Control	1.53
11	Physics and Environment Security	1.30
12	Operational Security	1.26
16	Information Security Incident Management	1.20

After analysis and evaluation of the security of information systems in the field of Department DISKOMINFO Depok City, here are still many who do not follow the standards of information security.

Formulation of Recommendations

Based on the findings of the analysis and evaluation of the security of information systems then compiled recommendations for improvements to the conditions in the field of Data and Information DISKOMINFO Depok are not in accordance with the procedure. Some recommend namely:

1. Provide training and education programs to all employees and information data fields.
2. Assets related to information and information processing facilities on the Field Data and Information to be identified and inventoried right, and information assets must be properly maintained. Asset inventory must be accurate, up to date and consistent.
3. Field Data and Information DISKOMINFO Depok should make the rules on access control
4. Safe area must be protected by appropriate physical entry controls to ensure that only authorized personnel are allowed to enter.
5. Field Data and Information DISKOMINFO Depok should establish policies prohibit the use of unauthorized software

IV. **CONCLUSION**

1. Identify the level of security risk in this research by looking at the matrix level of risk, identification is divided into three levels: high risk, medium risk and low risk, such as mail servers and Information System for Budget Transparency (SITRA) (high risk) , desktop and application Depok Transport Direction (medium risk), printer and scanner (low risk).
2. Control of information security risks to be performed on the Field Data and Information DISKOMINFO Depok City with an objective selection and control of information security controls.
3. Planning Information Security Management System (ISMS) is using the standard ISO 27001: 2013 and the assessment of the level of maturity (maturity level) using the System Security Engineering Capability Maturity Model (SSE-CMM). Future studies could use another maturity model for comparison, such as the Capability Maturity Model Integration (CMMI).

REFFERENCE

[1] R. Sarno and I. Iffano, *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. Surabaya: ITS Press, 2009.

[2] S. T. Arnason and K. D. Willett, *How to Achieve 27001 Certification: An Example of Applied Compliance Management*, vol. 28. 2007.

[3] ISO, "International Standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements," *Iec*, vol. 27001, no. 27001, 2013.

[4] CMU, "System Security Engineering Capability Maturity Model (SSE-CMM)," *Proc. 19th Int. Conf. Softw. Eng. ICSE 97*, vol. 35, pp. 566–567, 2003.

[5] Razieh Sheikhpour and Nasser Modiri, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Control", International Journal of Security and Its Applications, Vol. 6, No. 2, April, 2012

[6] Wolfgang BOEHMER, "Cost-Benefit Trade-Off Analysis of an ISMS based on 27001", International Conference on Availability, Reliability and Security, January 2009

[7] Heru Susanto, Mohammad Nabil Almunawar and Yong Chee Tuan, "Information Security Management System Standards: A Comparative Study of the Big Five", International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05