A Maturity Level Framework for Measurement of Information Security Performance

Rosmiati
Universitas Islam Indonesia
Yogyakarta, Indonesia

Imam Riadi
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Yudi Prayudi
Universitas Islam Indonesia
Yogyakarta, Indonesia

ABSTRACT

Information is one of the most important assets of the company. With the development of information technology is very rapid, the possibility of ever increasing information security disorder. This research was conducted to find out the level of information security in organization to give recommendations improvements in information security management at the company. This research uses the ISO 27001 by involving the entire clause that exists in ISO 27001 checklist. The source of the data used in this study was a detailed questionnaire and interview. The respondents in this study are all the employees are in the Office of the Bureau of information technology as many as 14 peoples. The results showed maturity level of information security in the Office of the Bureau of information technology is at level 2. The value of the gap between the value of the maturity level of the current and expected level of maturity value is 2.79. Recommendations for improvement are given requires an understanding of the company and also required coordination with the internal company.

Keywords

Information, Security, ISO 27001, Maturity Level, Value Gaps

1. INTRODUCTION

Some companies do not hesitate invest their share in the fields of Information Technology (IT), although the investment make enermous drain to budget. This is done as an effort to get the convenience and benefits of the use of IT., which is expected to help the performance of the company to conduct a competitive business strategy[1]. And Information technology is a very important requirement for all enterprise organizations because it is proved to help in improving the effectiveness and efficiency of enterprise business processes [2].

Assessment and evaluation of investments that have been issued for the implementation of IT is proper to be considered. Based on some research explained that the company has begun to realize and start doing performance measurement and evaluation [1]. In the analysis of information technology, there are several frameworks that refers to the reference international information technology governance that has been widely accepted and proven implementation such as ISO 27001, COBIT, ITIL and so on [3], which can be implemented in accordance with the conditions of different companies.

At the heart of information technology, information security aspects play a vital role and are thus becoming central issues in those systems effective usage [3]. ISO 27001 is a reference method/framework for measurement and control of information security [4].

XYZ company as an experienced provider of port services, helped spur economic growth by providing services and port services, especially in the eastern region of Indonesia as well as a mean for businesses to expand their business. Given the number of services performed by XYZ company is required of information security to information the company to improve customer satisfaction. Therefore it is necessary to assess the level of maturity of the security of information on XYZ company. At XYZ company, has never been done for security performance measurement information so that needed measurements to determine the condition of the implementation of information security at XYZ Company.

2. LITERATURE REVIEW

2.1 Information Security

Information security is the preservation of information from all possible threats in an attempt to ensure or ensure business continuity, minimize business risk, and maximize or accelerate return on investment and business opportunities[6].

Information security has some aspects that must be understood to be able to implement it. Some of these aspects, the first of three that are most commonly named C.I.A triangle model, as shown in Figure 1[4].

Confidentiality
Information Security Aspects
Integrity
Availability

Fig 1 Aspects of Information Security

Confidentiality, integrity and availability are basic requirements for business information security and provide the maintenance requirements of the business [3][4].

- Confidentiality (C): All information must be protected according to the degree of privacy of their content, aimed at limiting its access and used only by the people for whom they are intended;
- Integrity (I): All information must be kept in the same condition in which it was released by its owners, in order to protect it from tampering, whether intentional or accidental;
- Availability (A): All the information generated or acquired by an individual or institution should be available to their users at the time they need them for any purpose;

2.2 Control Objectives For Information andRelated Technologi (COBIT)

COBIT is a high-level IT governance and management framework. It focuses on the broader decisions in IT management and does not dwell into technical details. It is a framework of best practices in managing resources, infrastructure, processes, responsibilities, controls, etc [1][2][5][7][8].

COBIT contains 34 IT processes, each with high-level control objectives (COs) and a set of detailed control objectives (DCOs). In total, there is a sum of 318 DCOs defined for these processes.It is a good solution when managers are looking for a framework which serves as an integrated solution within itself, rather than having to be implemented along with other IT governance frameworks.

However, its biggest short-coming is that it does not give “howto” guidelines to accomplish the control objectives. This is not preferred when the thrust in on correct implementation of security controls.

2.3 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector. ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. ITIL presents a broad set of management procedures, which apply to all aspects of IT infrastructure, with which an organization can manage its IT operations (Zegers, 2006, Wegmann, 2008)[3].

The ITIL consists of five publications, each providing guidance on a specific phase in the service management lifecycle. The ITIL Core publications are as follows:

- Service strategy
- Service design
- Service transition
- Service operation
- Continual service improvement

ITIL can help companies assess their risks, and put procedures in place to log and respond to incidents. ITIL, and more specifically the ITIL security management process, is widely used for the implementation of information security within an organization. ITIL has placed the information security management process within the Service Design core practice book. The goal of the information security management process is to align IT security with business security and ensure that information security is effectively managed in all services and service management activities (OGC, 2007; Taylor,2008)[3].

2.4 ISO 27001

ISO 27000 series is a family of IS management standards. It is the set of standards in this family that focuses on Information Systems Management (ISM). Initially known as the BS7799 standard, this was included in the set of ISO standards when ISO decided to include ISMS standards as one of the set of ISO standards. As a result of this, the standards' name/number was adopted and it was called the ISO17799:2005 series [5]. ISO 27001 published in 2009 and is Indonesia's version of ISO/IEC 27001:2005, contain specifications or requirements that must be met in developing information security management system (ISMS)[9].

ISO 27001 defines methods and practices of implementing information security in organizations with detailed steps on how these implemented. They aim to provide reliable and secure communication and data exchange in organizations. Also, it stresses on a risk approach to accomplishing its objectives[5]. This standard is independent of information technology products require the use of risk-based management approach, and is designed to ensure security controls have been able to protect the information assets of various risks and give confidence level of security for interested parties[4]. Table 1 illustrates a comparison between COBIT, ITIL and ISO 27001.

Table 1. Number of Area ISO 27001

Focus	Implementation of security controls, stress on risk—management approach
Paradigm	Information Security Management System
Scope	Standard documents or information security management system ISMS (Information Security Management System), which gives scope for the process of evaluating, implementing and maintaining information security by "bestpractice" in information security
Structure	11 sections with 36 objective which are further divided into sub objective
Guide	Instructions for the implementation of Information Security as Care Information in order to ensure business continuity, minimizing business risk and optimize business and investment opportunities
General Use	implementation of the Information Security Management System (ISMS)
Certification	Is certifiable

The organizational structure of ISO / IEC 27001 is divided into two major parts:

- Clause: Mandatory process

Clause (Article) is a requirement that must be met if the organization implements ISMS using standard ISO / IEC 27001

- Annex A: Security Control

Annex A is a reference document that is provided and can be used as a reference to determine what security controls (security control) that need to be implemented in the ISMS, which consists of 11 security control clauses, 39 control objectives and 133 controls.

The standard states the main requirements that must be met regarding:

1. Information security management system (framework, processes and documentation)
2. Management responsibility
3. Audit internal ISMS
4. Manajemen reviewing the ISMS

5. Continuous Improvement

Besides the main requirements above, this standard requires goal setting controls and information security controls include 11 area security as follows:

1. Information Security Policy
2. Organization of information security
3. Asset Management
4. Human resources regarding information security
5. Physical and environmental Security
6. Communications and operations management
7. Access control
8. The procurement/acquisition, development and maintenance of information systems
9. The management of information security incidents
10. Business Continuity Management
11. Compliance

2.5 SSE-CMM

SSE-CMM is the Capability Maturity Model (CMM) for System Security Engineering (SSE). CMM is a framework for developing the process, such as the technical process of both formal and informal. SSE-CMM consists of two parts, namely:

1. The Model for process security techniques, projects and organizations, and
2. Assessment methods to know the maturity process.

SSE-CMM has five levels of ability to demonstrate the level of maturity of the process.

- Level 0 indicates not all base practices are performed.
- Level 1 indicates all the base practices are performed but informally, meaning that there is no documentation, no standards and is done separately.
- Level 2 planned & tracked which indicates commitment planning process standards.
- Level 3 well defined meaning standard process has been run in accordance with the definition.
- Level 4 is controlled quantitatively, which means improved quality through monitoring of every process.
- Level 5 is improved constantly indicating the standard has been perfect and the focus to adapt to changes.

SSE-CMM method used by giving the score assessment on each area of the process that selected between 0 to 5 for each process area[10].

2.6 Maturity Level

One of the tools of measurement of the performance of a system of information system is a model of maturity level[1]. Maturity model for management and control in the process of information system based on the evaluation methods of the Organization so that it can evaluate himself from level 0 (none) to level 5 (optimistic). Maturity model is intended to determine the existence of the problem and how to determine the priority of improvement.

Results of calculating the value of the maturity level is maturity index to obtain the level of maturity in accordance with Table 2[8].

Table 2 Maturity Level Assessment Criteria

Maturity Index	Maturity Level
0 – 0.49	0 – Non Existent
0.51 – 1.50	1 – Initial / Adhoc
1.51 – 2.50	2 – Repeatable But Intutive
2.51 – 3.50	3 – Defined Process
3.51 – 4.50	4 – Managed and Measurable
4.51 – 5.00	5 - Optimized

Descriptions measurement techniques are made by the nominal size to sort objects from the lowest to the highest, these measurement only give the order rank. Measurements were carried out directly from values that refers to the values of the exiting sorting in maturity models as show in Table 3 [2].

Table 3 Maturity Level

0 Existent	The company does not care about the importance of information technology to be managed either by the management
1 Initial	Company reactively perform application and implementation of information technology in accordance with the needs of existing sudden, without preceded by prior planning.
2 Repeatable	The Company has a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency.
3 Define	The Company has had a formal and written standard operating procedures that have been socialized to all levels of management and employees to be obeyed and worked in daily activities.
4 Manage	The company has had a number of indicators or quantitative measures that serve as targets and objective performance of every application of information technology applications.
5 Optimized	The Company has implemented the information technology governance refers to "best practice"

3 RESEARCH METHODS

This chapter describes how research where there are details about the material or the materials, tools, sequence of steps to be made in a systematic, logical so it can be used as guidelines are clear and easy to resolve the problems, analysis of results and the difficulties encountered. The sequence of steps problem solving research can be seen in Figure 2.

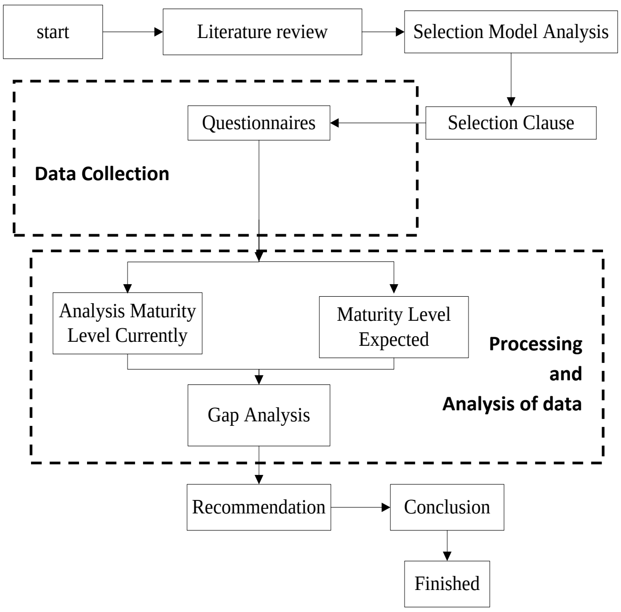

Fig 2 Research Methodology

In this study, the data can be processed from the questionnaiers by respondents are filled according to the data by means of questionnaires, while data is not in accordance with the instructions questionnaires will not be processed further.

Based on the questionnaire that was distributed to respondents selected for filling out the questionnaire in this study were 14 respondents. The software used for data processing by using Microsoft Excel software.

Tabel 4 Respondents

No.	Functional Structure of IT Bureau XYZ company	Number
1	Head of Information Technology Bureau	1
2	Assistant bureau chief of information technology Development of Systems & Applications	1
3	Assistant bureau chief of information technology for Data & Information	1
4	Assistant bureau chief of information technology Field Support System	1
5	Senior Analyst Data and Information	1
6	Senior Analyst Data and Information	1
7	CPDMT System Administrators and Database	1
8	Senior executor Support Systems and Networks	1
9	Programmer	3
10	Senior Executing Data Processing and Reports	1
11	Junior Analyst Data and Information	1
12	Executing Administration Information System	1

4 RESULTS AND ANALYSIS

This section discusses the results of the analysis are performed against what is retrieved, reviewed on quantitative and qualitative. Data analysis includes the implementation and performance measurement of the level of maturity against the security of the information in the Office of the Bureau of information technology XYZ company The data obtained from the results of the questionnaire and the interview is treated in accordance with ISO/IEC 27001.

4.1 Summary Of The Maturity Level

The repondents calculation summary per clause by using descriptive calculation formula obtained result as shown in Table 5.

Tabel 5 Summary of The Value Maturity Level

No	Clause	Index	Level
1	5	2.68	3
2	6	2.18	2
3	7	1.91	2
4	8	2.19	2
5	9	2.09	2
6	10	2.10	2
7	11	2.02	2
8	12	2.31	2
9	13	2.03	2
10	14	2.50	3
11	15	2.29	2
Average		2.21	2

The results of the calculation to get the average value of the information security controls on XYZ company of 2.21. From this value we can conclude that the security information are on the second level, ie repeatable but intuitive. Based on the result from Table 5, for each process in the clause, it obtained graphs as in the Figure 5 below.

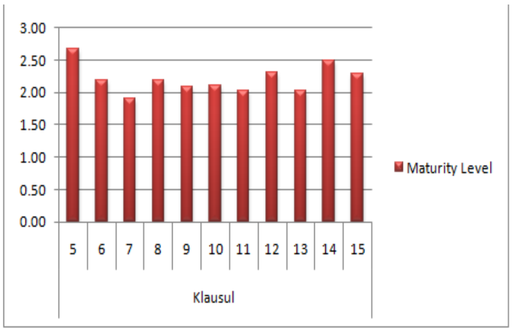

Fig 3 Measurements graphs in maturity level

4.2 The Gap of Value Maturity Level

After knowing the maturity level of information security is currently at 2.21 (Repeatable but intuitive) and the expected maturity level is 5 (Optimized). The reason the value to be achieved by 5 is the readiness of the company in the field of security policies, procedures and processes, and access control information security. Maturity Level gap can be seen in Table 6.

Table 6 Maturity Level Gap

Clause	Maturity Level		
	current	*expected*	*Gap*
5	2.68	5.00	2.32
6	2.18	5.00	2.82
7	1.91	5.00	3.09
8	2.19	5.00	2.81
9	2.09	5.00	2.91
10	2.10	5.00	2.90
11	2.02	5.00	2.98
12	2.31	5.00	2.69
13	2.03	5.00	2.97
14	2.50	5.00	2.50
15	2.29	5.00	2.71
Average			2.79

Based on Table 6, the distance gap between the current conditions with the expected conditions for each clause is a clause 5 no values gap of 2.32. Value gaps to Clause 6.7 and 8 each worth 2.82, 3.09 and 2.81. Clause 9.10 and 11 each gap value is 2.91, 2.90 and 2.98, while clause 12, 13, 14 and 15 respectively to get the value gap of 2.69, 2.97, 2.50 and 2.71. After getting the value gap for each clause then all values are summed gap then averaged to obtain the value of the overall gap. Overall value of the gap there is a distance of 2.79 between the maturity of the current conditions with the maturity of the expected conditions. There are fairly large gap, then the required adjustment of each control. Recommendations will be given to each control so much focus on the improvement of weak controls. Value ratio of the current maturity level and the value of the expected maturity level is depicted in Figure 4.

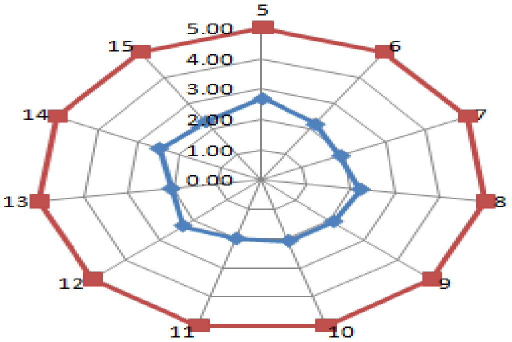

Fig 4 Comparison Value Maturity Level Current and Expected

In Figure 4 illustrates the value of the current maturity level of the lowest contained in Clause 7 with a value of 1.91 so that the value gap (the gap) between the value of the current maturity level with the maturity level in this clause at 3.09 (the value of the gap is highest). While the value of the current maturity level that is highest in Clause 5 with a maturity level value of 2.68, so that the value of the gap in this clause at 2.32 (the lowest value of the gap). Thus the higher the value gap clause, the more likely the clause is to get a security breach and the lower value of the gap in clause then the less likely the clause is to get security problems.

5 FINDING AND IMPROVEMENT STRATEGY

Based on the analysis that has been done in the Bureau of Information Technology Company, the values of the findings will be matched to the conditions of maturity for each control ISO 27001 results were found the following problems:

1. A confidentiality agreement has not been described in detail and specific
2. Has not done the review and renewal of access rights on a regular basis. Renewal of the permissions are not required on a regular basis.
3. There is no return on the assets of the company by employees, contractors or third party after quitting the company or transferred any other part.
4. Many operating procedure are not documented, that the recovery procedure, program start-up, close-down, back up, restart the system, maintenance scheduling, fault handling instructions, and restrictions on the use of system facilities.
5. Lack of awareness of employees and third parties in the division of tasks and responsibilities
6. There is no control and physical protection by employees of the media information system.
7. There has been no formal authority to process the information before it opened to the public
8. Rules and access control permissions to each user or group of users is not clearly stated in a policy statement about access rights
9. Employees less attention to security weaknesses in the system as well as service and attention to key corporate data to be protected from loss, damage and forcing.

Based on the findings obtained from the analysis of security information then compiled recommendations for improvement of the condition of the company. Some recommendations are:

1. Describe in detail the confidentiality agreement and specifically including maintaining the confidentiality of the password
2. Reexamination of the access rights of each and updating access rights in case of transfer of part or advancement in accordance with their respective access rights.
3. Every employee, contractor or third party should return all the company's assets used for work depending on the contract, when the employee, contractor or third party quit the company or moved other part.
4. Operating procedures specified in the security policy should be documented and maintained. The surgical procedure should be treated as formal documents and changes authorized by management.
5. Make a division of tasks in order to reduce the possibility of the risk of incident or abuse of the system by accident. Should be considered the separation of the management or execution of certain duties and responsibilities, to reduce the chance of modifying without permission or abusive information or services.

6. Media information systems should be controlled and physically protected to prevent damage to assets and interruption to business activities. Appropriate procedure should be established to protect documents, computer media, the data input / output and documented system from damage, theft and unauthorized access.

7. Attention should be given to protect the integrity of electronically published information to prevent modifications that may harm the company's reputation. The information provided to the public, such as information on the web that can be accessed via the internet must be in accordance with the laws, rules, and regulations in the jurisdiction

8. The business requirements of the access control must be established and documented. Access control rules and rights for each user or group of users should be clearly stated in a policy statement about access

9. All employees, contractors and third party users of information systems and services should be required to record and report any allegations or findings of security weaknesses in the system or the services. This aims to ensure that information security events and weaknesses detection of information security can be dealt with in a timely and correct.

6 CONCLUSION

The results obtained from the measurement of the level of maturity for information security in the field of information technology bureau at XYZ company is level 2 (repeatable but intituive). Results of the questionnaire management to obtain an average value for all of the clauses is 2:21 range of 0 to 5. And the value of the gap between current security conditions and the condition of the expected 2.79. From this value can be concluded that the security information on the second level, is repetitive but intuitive. Thus the results of the analysis means that the procedure contained in the delivery and support of control have been developed in the process to handle the task, and followed by everyone involved. No training and communication of standard procedures. The responsibility for implementation handed over to each employee. Employee confidence is very high, so that errors may occur

7 FUTURE WORK

The information system security audits using the ISO 27001 standard and maturity level assessment using the SSE-CMM, because the ISO does not have the methods of assessment and therefore for the development of further research can use other maturity models for comparison

.

8 REFERENCES

[1] Herison Surbakti,"Cobit 4.1 A maturity Level Framework for Measurement of Information System Performance (Case Study : Academic Bureau at Universitas Respati Yogyakarta)", International Journal of Engineering Research & Technology (IJERT), Vol. 3, Agustus 2014, ISSN:2278-0181, pp 999 – 1004.

[2] Surni Erniwati and Nina Kurnia Hikmawati, "An Analysis of Information Technology on Data Processing by using Cobit Framework", (IJACSA) Intermasional Journal of Advanced Computer Science and Application, Vol. 6 No. 9 2015, pp 151 – 157.

[3] S. Faris, H. Medromi, S. El Hasnaouni, H. Iguer and A. Sayouti, "Towards an Effective Information Security Risk Management of Universities Information Systems Using Multi Agent System, Itil, Iso 27002, Iso 27005", (IJACSA) Intermasional Journal of Advanced Computer Science and Application, Vol. 5 No. 6 2014, pp 114 – 118.

[4] Riyanarto Sarno and Irsyat Iffano, "Information Security Manajemen Syytem", Surabaya: ITSPress 2009 (in Indonesian Language).

[5] Varun Arora, "Comparing Different Information Security Standarts : COBIT vs ISO 27001, Carnegie Mellon University, Qatar.

[6] Ermana, F. H., Tanuwijaya Mastan, I. "Security audit information system based on the ISO 27001 Standards on PT. BPR Jatim". STIKOM. Surabaya. 2012.

[7] Karim Youssfi, Jaouad Boutahar and Souhail Elghazi, "A Tool Design of COBIT Roadmap Implementation", (IJACSA) Intermasional Journal of Advanced Computer Science and Application, Vol. 5 No. 7 2014, pp 86 – 94.

[8] Gusti Ayu T K, I Made Sukarsa and I Putu Agung B, "Governance Audit of Application Procurement Using Cobit Framework", Journal of Theoretical and Applied Information Technology (JATIT)". Vol 59. No.2. ISSN:1992-8645.2005, pp 342 – 351.

[9] Indonesian national standard. Information Technology - Security Techniques - Information Security Management Systems - Requirements (ISO / IEC 27001: 2005) (in Indonesian Language).

[10] Adi Supriyatna. "Analysis of the academic information system security level by combining Standard BS-7799 with SSE-CMM", Prosiding Seminar Nasional Aplikasi Sains & Teknologi (SNAST), ISSN: 1979-911X,Yogyakarta, November 2014.

[11] Rozas, IS, Sarno R. "SiPKoKI ISO 27001: Electoral System Of Information Security Controls Based ISO 27001", Seminar Nasional Pascasarjana XI-ITS, Surabaya, Juli 2011.