Data Center Governance Information Security Compliance Assessment Based on the Cobit Framewok

(Case Study The Sleman Regency Data Center)

Andrey Ferriyan
Dept. Of Computer Science
Gadjah Mada University
Yogyakarta, Indonesia

Jazi Eko Istiyanto
Dept. Of Computer Science
Gadjah Mada University
Yogyakarta, Indonesia

***Abstract*—One of control domain of Cobit describes information security lies in Deliver and Support (DS) on DS5 Ensure Systems Security. This domain describes what things should be done by an organization to preserve and maintain the integrity of the information assets of IT where this all requires a security management process. One of the processes is to perform security monitoring by conducting periodic vulnerability assessment to identify weaknesses. Because Cobit is not explained technically, so it needs a method to utilize data that has been standardized. One of the standardized databases for vulnerability is CVE (Common Vulnerabilites and Exposures).This study aims to assess current condition of Data Center on Department of Transportation, Communication and Information Technology at Sleman Regency and assess the maturity level of security as well as providing solutions in particular on IT security. Next goal is to perform vulnerability assessment to find out which are the parts of the data center that may be vulnerable. Knowing weaknesses can help evaluate and provide solutions for better future. Result from this research is to create tool for vulnerability assessment and tool to calculate maturity model.**

Keywords—COBIT; CVE; maturity model

I. INTRODUCTION

Department of Transportation, Communication and Information Technology at Sleman Regency is one of the agencies that have the function of providing construction administration, development and management of communications network infrastructure. The agency has responsibility for managing the communications network infrastructure. In the development the infrastructure there are several incidents that have occurred. Several subdomain have been defaced by cracker. Distributed Denial Of Service (DDOS) attacking VoIP server. Remote security hole take place in the server where management authority not from Departemen of Transportation, Communication and Information Technology but the server itself lies on Data Center at Sleman Regency.

The evaluations from incidents conducted merely when there is a problem and the agency don't have evaluation planning and concept in safety evaluation in accordance with standards.

According to [1], to obtain a comprehensive security of the system, it is important to do the assessment and evaluate all aspects of the start of computer network security, application security, operating system security, database security, physical security and the environment.

Standard that can be used to assess the condition of governance data center is using the framework called Control Objectives for Information and Related Technology (COBIT). Today the use of Cobit framework is pretty much widely adopted and used as one of the standards in conducting research on the assets associated with information technology.

An application which can help an auditor is needed because not all applications can be applied in governance. Therefore, it needs to make an application that can be used to help a security auditor to evaluate the security of government information.

This paper describes how to assessing the data center using two methods. First by checking the compliance based on the Cobit framework and second by vulnerability assessment using tool combine with vulnerability standardized database.

II. LITERATURE REVIEW

Many have conducting research by presenting the results from the Cobit framework. However, Cobit to the security or vulnerability testing has been no detailed assessment. It's because Cobit is process oriented and works on management level. Comprehensive study conducted by comparing the level of maturity of the level of management. Cases studied tended to focus on one area, the management level or just the technical side.

According to [2], organization's management of IT governance requires the application of information technology environment to measure existing and planned in advance. Focus research only on management side and not technical issues where this is not much different from what is done by the [3] in his study.

According [3], vulnerabilities occur in the object under study is more to human error as an error in the conduct of data input, data duplication, deletion is done illegally, the absence of data storage settings, the absence of a recovery strategy the

data in the event of damage and others. The focus of research is over the control of the management and assessment of existing conditions.

Contrast to [3] where the focus of their research is more to the technical side. It mentions that the weakness of the system is classified into several pieces which are application vulnerabilities, network vulnerabilities, and host vulnerabilities. Research can not be considered comprehensive because it is merely checking individual.

Research conducted by [4] can help the system administrator to find configuration errors and then will be adjusted so that there is an error can be corrected. However, there is still a shortage of which is a new environment can be checked only one type only the server-based server Apache, PHP, MySQL.

As [5] who did research on the classification of network vulnerabilities with a research focus on the signs of the attack resulting from a firewall or IDS devices. Measuring threat approach to estimate the effects of attacks that occur in a computer network. It's utilizing the Common Vulnerability Scoring System (CVSS) to measure the amount of threat generated in the event of an attack.

III. Research Methods

Steps in research can be seen in Figure 1.

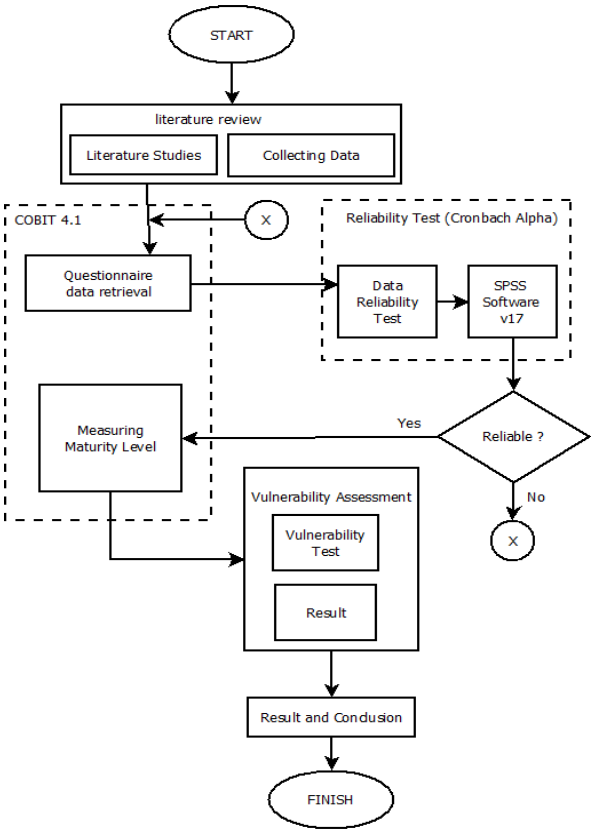

Fig. 1. Research steps

There are two methods conducting this research as described before. First by checking the compliance using Cobit. Cobit has a method to calculate maturity model how far the data center by looking at the security management process. In what level security management has been running well. Cobit will calculate it from level 0 to level 5. Of course this doesn't mean level 5 is very secure but by following it and using proper procedure we are convinced that the security management process run in accordance with the applicable procedures as stated by Cobit framework.

A. Literature Review

Studying literatur review of research related to Cobit and vulnerability assessment. Data collection was conducted by collecting technical documentation related to the data center like IP addresses, type of operating system, UNIX-like or Windows.

B. Questionnaire and Data Reliability

Questionnaires were distributed to the staff of the department. The questionnaire was taken from COBIT 4.1 Deliver and Support (DS) 5 Ensure Systems Security. Before the result from questionnaire can be used, its necessary to test the reliability first. Testing data reliability using Cronbach Alpha formula. Cronbach Alpha using scale from 0 to 1. If result from the formula equal or more than 0.6 then data considered reliable. Result from reliable data can be used to calculate maturity model. Based on the analysis, a tool for calculate of maturity model and a tool for vulnerability assessment are needed.

Vulnerability assessment tool will use CVE as standardized vulnerability database. The tool will use binary parsing to parse binary file within servers. If the version from binary version match from CVE list then it is considered vulner.

C. Implementation

Implementation from maturity model tool consists of :

- Reliability test to determine the level of reliability of measurement before continuing on maturity model calculations.
- Calculation of maturity analysis generated after the existing questionnaires obtained from the respondents.
- Reliability test to determine the level of reliability of measurement before continuing on maturity model calculations.

Implementation from a vulnerability tool consists of :

- Collecting binary version from all of servers.
- Comparing between binary version and CVE list. If matched then its considered vulner.

IV. Result and Discussion

After the tool is made, tests were done on two aspects, first the maturity of model-based testing, second testing from six servers that reside in the data center.

A. Maturity Model Testing

Maturity model test at the Department of Transportation, Communication and Information can be seen in Table 1

TABLE I. RESULTS OF MATURITY MODEL TESTING

Maturity Level	**All Questions**	**Total Question**	**Maturity Value**	Maturity Value Normalization	Maturity Model
Non Existent	5	7.5	1.5	0.044	0
Initial	6	35.5	5.917	0.175	0.175
Repeatable	8	60	7.5	0.222	0.444
Defined Process	7	46.5	6.643	0.197	0.591
Managed and Measureable	12	66	5.5	0.163	0.652
Optimised	10	67	6.7	0.198	0.99
Total			33.76	1	**2.852**

Table 1 shows that the value of the maturity model 2,852 value means the value at level 2.

B. Testing Vulnerability On Six Servers

The test is performed to determine the extent of the servers in the data center experienced technical vulnerabilities. This can be shown in Table II.

TABLE II. THE RESULT OF TESTING VULNERABILITY

No	Server Name	Severity Low	Severity Medium	Severity High	Total Vulnerability
1	Slemankab.go.id	3	0	2	5
2	Subdomain Slemankab	1	0	0	1
3	Web Perijinan	3	0	2	5
4	Database Perijinan	3	0	2	5
5	Web LPSE	0	1	1	2
6	Database LPSE	2	3	2	7
	Total	12	4	9	25

V. CONCLUSION AND SUGGESTIAN

A. Conclusion

Based on the test results that have been obtained, it can be concluded:

- The result of the questionnaire maturity model calculations COBIT 4.1.
- Maturity Model from Deliver and Support domain 5 shows the maturity value of the model is 2.852 for the Department of Transportation, Communication and Information.
- The results of the model calculation of maturity levels reached by the Department of Transportation, Communication and Information Technology is a level 2 or Repeatable for current conditions.
- Tools are made to calculate the maturity model has been proved correct by manual calculation using the formula in a spreadsheet.
- Tools are made to perform security testing failed to detect the presence of several vulnerabilities found in servers are tested.

B. Suggestion

The research using two methods has limitations that can be used as a reference for future development, suggested few things:

1) As for method one, for further testing maturity model involves calculating the expected maturity attributes such as awareness and communication, policy standards and 6 procedures, and automation tools, skills and expertise, responsibility and accountability and goal setting and measurement .

2) The necessity of making plans related to IT security and the solution where these plans appear based on the analysis of existing risks.

3) Scheduled for reporting security either in the form of a log or chart that can be read in conjunction with the existing security conditions both recent and in the distant past .

4) As for method two, PyCVE tool or script that is used in the research is still need to improve because not all application recorded on listing_file.txt readable version due to limitations in parsing binary file.

5) The tool for vulnerability assessment need more accurate in mapping for easier find any applications that may be vulnerable to later do an update on the server

REFERENCES

[1] Sayana, S., A., 2003, Approach to Auditing Network Security, Information Systems Control Journal Volume 5

[2] Lainhart IV, J., W., 2000, CobiT : A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities, Journal Of Information Systems

[3] Pribadi, Y., I., 2011, Penilaian Kondisi Kini Tata Kelola Data Kependudukan Pada Aspek Pengelolaan Data Dengan Menggunakan Kerangka Kerja COBIT (Studi Kasus Kota Pontianak), Tesis, Jurusan Ilmu Komputer FMIPA, UGM, Yogyakarta.

[4] Eshete, B., Villafiorita, A., and Weldemariam, K., 2011, Early Detection of Security Misconfiguration Vulnerabilities in Web Applications, In Proceedings of the 6th Conference on Availability, Reliability and Security (ARES2011), Vienna, Austria, 169-174

[5] Xi, R., Yun, X., Jin, S., dan Zhang, Y., 2011, Network Threat Assessment Based on Alert Verification, PDCAT 2011 Proceedings of the 2011 12th International Conference on Parallel and Distributed Computing, Applications and Technologies, Gwangju, Korea, 30-34