IOP Conf. Series: Materials Science and Engineering **879** (2020) 012047 doi:10.1088/1757-899X/879/1/012047

Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013

G G Prapenan[1], G C Pamuji[2]
[1,2]Master of Information System, Faculty of Postgraduate, Universitas Komputer Indonesia, Indonesia

Email : galihdrm@gmail.com

Abstract. Information system security is now very important to prevent from an attack. Besides that, low level security can harm the productivity of an organization. The purpose of this research is to ascertain and know the level of information system security in XYZ Company, because it has never conducted an audit information system security. In this research, it used the COBIT 5 framework to audit information security management system in a company based on the ISO 27001 standard. This audit was conducted to identify information system security that was not good. In addition to improving the information security management system that will be adjusted to the ISO 27001 standard. This research was composed by applying a qualitative methodology, observation of the activity in the company and reviews related information security management system literature document existing. For the auditing using COBIT 5 framework, audit focuses on four kinds process that consists of APO12, DSS05, MEA02 dan EDM03. The audit COBIT 5 two results in consisting of "Managed Process" Level on APO12, MEA02 and EDM03 and "Performed Process" level on DSS05. The resulting of this research will be used a reference to the improvement of existing information system security in the company.

1. Introduction

Currently, the security of information systems is now very important to prevent from an attack, besides that low security can threaten the productivity of an organization [1-5]. XYZ Company is a manufacturing company that produces a variety of fabrics. In the company, there are several information systems to support business activities. However, the information security management systems has never been done since the company was founded. It should be for this XYZ company that has been established for more than twenty years and has quite a lot of employees already know the level of information system security, thus after knowing the level of security of the company's information system can be used as a reference to improve the security of information systems that can minimize the occurrence of threats or also later the company wants to plan to get an ISO certificate of information security management system. Because information is a valuable asset in an organization [1], therefore in storing information require to have a good information security management system to secure the information [4]. Now this XYZ Company needs a process analysis to find out the information security management system that has been fulfilled with COBIT 5 and ISO 27001 in information technology security aspects.

In building information systems security management must have the main criteria and requirements following the standards [2][3]. In addition, good governance of information system security will improve system performance. While ISO 27001:2013 international standards for work

system specifications are requirements for system reliability and system accuracy that will protect information security in the company [6-9].

Based on the research objectives, researchers will conduct an audit to evaluate the information security management system and some security activities using COBIT 5. COBIT 5 will be applied for security management evaluations in general companies related to ISO 27001:2013 [1][2][5]. The purpose of this research is to ascertain and know the level of information system security in XYZ Company.

2. Methods

This research was composed by applying a qualitative methodology with several stages of research starting from 1) Research Planning, 2) specific the scope of analysis, 3) Data Collection and Processing, 4) Result Report Analysis, 5) Conclusions and Recommendations. To obtain information in this research, researchers involved 3 people consisting of Head of IT, IT Support Team and Developer Team.

To obtain data in this research, researchers conducted analysis and observation of company activities using the selected toolkit and for the questionnaire rating scale using a Likert scale [10] including 1) Very Poor, 2) Poor, 3) enough, 4) Good and 5) Very Good. For secondary data, researchers take data obtained from the previous research literature on information security management system audit using COBIT 5 and ISO 27001 taken from journals, papers, thesis, and articles. This reference can be a reference for researching companies that are in compliance with the existing information security management systems audit.

The COBIT 5 processes selected are APO12, DSS05, MEA02, and EDM03 [11]. The process chosen includes the scope to be observed regarding information security management systems. The COBIT 5 Process Assessment Model (PAM) has a high level of capability that will reach the highest level of capability. Each level in COBIT 5 PAM will be assessed based on ISO / IEC 15504. The scale consists of Not Achieved (N) with range 0% - 15%, Partially Achieved (P) with range 15% - 50%, Large Achieved (L) with range 50% - 85%, and Fully Achieved (F) with range 85% - 100% [9]. Based on the Table 1 below COBIT 5 the process capability model to assessment model [12].

Table 1. Cobit 5 Process Capability Assessment Model

COBIT 5 Process Capability Assessment Model (PAM)			
0	Incomplete Process	Performance Attribute (PA)	
1	Performed Process	PA 1.1	Process Performance
2	Managed Process	PA 2.1	Performance Management
		PA 2.2	Work Product Management
3	Established Process	PA 3.1	Process Definition
		PA 3.2	Process Deployment
4	Predictable Process	PA 4.1	Process Measurement
		PA 4.2	Process Control
5	Optimizing Process	PA 5.1	Process Innovation
		PA 5.2	Process Optimization

3. Results and Discussion

3.1. COBIT 5 Mapping Proses

First of all, auditors do not use all 5 PAM COBIT domains because they have a very broad scope. Firstly, the auditor mapped the company vision and mission based on COBIT 5 Enterprise goals as the scope of the ISMS. The company have a vision and mission 1) be a company that is always innovating in its products and is always accepted in the national and international markets, 2) offer quality products

accordingly with international checking standards, making products according to market needs. After that, the auditor maps the IT goals that are adjusted to COBIT 5. The auditors map the COBIT 5 IT to the COBIT process 5. Thus, that the mapping of the company Enterprise goals with the COBIT 5 process is found [13-15]. The audit will choose IT goals that are appropriate to its scope, but the audit only focuses on information security management system, thus that auditors only choose those that are related to the information security management system. After the process of mapping from the company vision and mission to the enterprise goals, the results of the process showed that the company's vision and mission did not meet with EG-6, EG-8, EG-14 and EG-17.

3.2. COBIT 5 Domain Selection

Based on the mapping between the IT-Related goals to COBIT 5 process, the selection of the appropriate COBIT 5 process related to the IT goals was achieved. The auditor only selected several primary (P) processes that are seemed suitable and needed in the company. Due to the very short time, this study audited only 4 domains regarding the information security management system. The auditors chose the APO12, DSS05, MEA02 and EDM03 domains from COBIT 5 PAM toolkit which a priority higher based on primary (P) relationship.

3.3. COBIT 5 Process Result

Based on the results of an audit using COBIT 5, this study obtained results for the management of enterprise information systems security in shown Table 2.

Audit results for Manage Risk (APO12) produce a capability value of 2.08, Manage Security Services (DSS05) produce a capability value of 1.75, Monitor, Evaluate and Assess the System of Internal Control (MEA02) producing a capability value of 2.08 and Ensure Risk Optimization (EDM03) producing a value of 2.00.

Table 2. Value of Capability Process

ID Process	Process Name	Result
APO 12	Manage Risk	2.08
DSS 05	Manage Security Service	1.75
MEA 02	Monitor, Evaluate and Assess the System of Internal Control	2.08
EDM 03	Ensure Risk Optimization	2.00
	Total	7.92
	Average	1.98

From each process that has produced capability value, overall, it has a value that is not much different except the process of Manage Security Service (DSS05) that results in a lower capability value than other processes.

In the process of assessing the capability level of the COBIT process, each process is checked in stages whether the process has met the requirements set at each level, starting from level 1 to level 5. Based on table 3 below, the results of the study of the capability level of each APO12, DSS05, MEA02, and EDM03 processes are all at level 1. However, for the APO12, MEA02 and EDM 03 processes the capability value has reached level 2, but little is achieved. Before the auditor conducts an internal audit, the auditor has determined the audit level limit at level 2. Based on the target process APO12, MEA02 and EDM03 achieve the target. On the other hand, the DSS 05 process has not reached the target and

only reached level 1. At this time, the research can assume that APO12, MEA02, and EDM03 have higher capability than DSS05.

Table 3. Process Capability Assessment Level Results

ID Process	Process Name	Process Capability Level					
		Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Align, Plan and Organize (APO)							
APO 12	Manage Risk	Fully Achieved	Fully Achieved	Not Achieved	Not Achieved	Not Achieved	Not Achieved
Deliver, Service and Support							
DSS 05	Manage Security Service	Fully Achieved	Large Achieved	Not Achieved	Not Achieved	Not Achieved	Not Achieved
Monitor, Evaluate and Assess (MEA)							
MEA 02	Monitor, Evaluate and Assess the System of Internal Control	Fully Achieved	Fully Achieved	Not Achieved	Not Achieved	Not Achieved	Not Achieved
Evaluate, Direct, and Monitoring (EDM)							
EDM 03	Ensure Risk Optimization	Fully Achieved	Fully Achieved	Not Achieved	Not Achieved	Not Achieved	Not Achieved

APO12, MEA02 and EDM03 reach level 2 that indicated will be processed performance management (2.1) which means that work will be carried out following the objectives and has not been achieved properly. Thus, that existing management may need to be improved following information security management system standards and implemented consistently. DSS05 reach level 1 that indicated Process Performance (1.1). Process performance is the process is implemented to achieve the objectives of the process

These results provide the level of activity in each domain, which aims to show the results of capabilities and level of the questionnaire results of the calculation capabilities of the previous stage and do a gap analysis (Table 4).

Table 4. Capability Gap

COBIT 5 Process	Capability Level Existing	Capability Level Target	Capability Gap
APO 12 - Manage Risk	2	2	0
DSS 05 - Manage Security Service	1	2	1
MEA 02 - Monitor, Evaluate and Assess the System of Internal Control	2	2	0
EDM 03 - Ensure Risk Optimization	2	2	0

3.4. Recommendation

Based on the results of internal audits involve APO12, DSS05, MEA02, and EDM03, recommendations can be taken to improve the information security management system that conforms to standards thus that capability levels can be increased.

For APO12, MEA02 and EDM03 processes are at level 2 but little is achieved. For full achievement at level 2 the company as follows, implementing, making plans, monitoring, and establishing precise controls regarding the information security management system. Thus, to measure the extent of the process that has been achieved based on testing and feedback from users as well as attachments related to information security management system thus that the information security management system can be managed well managed.

Similar to the previous approach, for the DSS05 process it can be upgraded to level 2 by achieving the following criteria: implementation, making plans, monitoring, and establishing controls regarding the management of information system security and evaluating the results of implementation. From there it can measure the process that has been achieved based on feedback from the user and the results of existing data. Thus, it can be more aligned with the management of information systems security by conducting quantitative analysis.

The above recommendations for each process are carried out to improve the information security management system based on COBIT 5 PAM which is aligned with ISO 27001 selected according to company requirements for level 2 capability index [9]. If a company is planning to get an ISO certificate, previously the company must improve the level in accordance with ISO 27001 standards, after that it can be made and asked to get an ISO certificate. If not, then the company can plan to reach the next level according to the indicators chosen regarding the information security management system.

4. Conclusion

Based on the results of the first audit process regarding information security management system using COBIT 5 adjusted to ISO 27001:2013 on XYZ companies that have "Performed Process" level 1 on DSS05 process and APO12, MEA02 and EDM03 only slightly reached the target but included "Managed Process" level 2 is based on a predetermined scope before the auditor conducts an internal audit and the auditor set on the target for the first time an audit of this company at level 3 for each selected COBIT 5 process.

Acknowledgment

We want to send gratefulness for XYZ company to conduct this research and we would like to thank very much the organizers of INCITEST 2020.

References

[1] Supriyadi, Y., & Hardani, C. W. 2018. Information System Risk Scenario Using COBIT 5 for Risk and NIST SP 800-30 Rev. 1 A Case Study. In *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)* (pp. 287-291). IEEE.

[2] Sinha, M., & Gillies, A. 2011. Improving the quality of information security management systems with ISO27000. *The TQM Journal*. **23**(4), pp. 367-376.

[3] Susanto12, H., Almunawar, M. N., & Tuan, Y. C. 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, ***11***(5), pp. 23-29.

[4] Fajar, A. N., Christian, H., & Girsang, A. S. 2018. Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. In *Journal of Physics: Conference Series* **1090(**1), p. 012060. IOP Publishing.
[5] Wahyudi, A. A. E., Ayu, D., & Aryani, N. W. S. Security Management Analysis of Security Services Using Framework COBIT 5 Domain DSS05. *International Journal of Engineering and Emerging Technology*, ***2***(2), pp. 37-40.
[6] Simbolon, N., & Hardiyanti, D. Y. 2019. Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013. In *Journal of Physics: Conference Series* **1196(**1), p. 012033. IOP Publishing.
[7] Susanto12, H., Almunawar, M. N., & Tuan, Y. C. 2011. Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, ***11***(5), pp. 23-29.
[8] Suminar, S. 2014. Evaluation of information technology governance using COBIT 5 framework focus AP013 and DSS05 in PPIKSN-BATAN. In *2014 International Conference on Cyber and IT Service Management (CITSM)* (pp. 13-16). IEEE.
[9] Laksono, H., & Supriyadi, Y. 2015. Design and implementation information security governance using Analytic Network Process and cobit 5 for Information Security a case study of unit XYZ. In *2015 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 1-6). IEEE.
[10] Septian, R. F., & Pamuji, G. C. 2019. Risk Analysis of Dutch Healthcare Company Information System. In *IOP Conference Series: Materials Science and Engineering* **662**(2), p. 022041. IOP Publishing.
[11] Putra, I. N., Hakim, A., Pramono, S. H., & Tolle, H. 2017. Adopted COBIT-5 Framework for System Design of Indonesia Navy IS/IT: An Evaluation. *International Journal of Applied Engineering Research*, ***12***(17), pp. 6420-6427.
[12] Arief, A., & Wahab, I. H. A. 2016. Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia). In *2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)* (pp. 388-392). IEEE.
[13] Huygh, T., De Haes, S., Joshi, A., & Van Grembergen, W. 2018. Answering key global IT management concerns through IT governance and management processes: A COBIT 5 View. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
[14] Trianto, W. 2018. Evaluation of Patient Information System in Public Health Service Using the COBIT 5 Framework. In *IOP Conference Series: Materials Science and Engineering* **407**(1), p. 012166. IOP Publishing.
[15] Bharaditya, I. W. P., Sukarsa, I. M., & Buana, P. W. 2017. Internal control improvement for creating good governance. *International Journal of Information Engineering and Electronic Business*, ***9***(3), p. 9.