eJAICT
ISSN 2355 1771
JOURNAL OF APPLIED INFORMATION, COMMUNICATION AND TECHNOLOGY
Published by:
Research Center of Technology and Innovation
Academic Research and Community Services
Swiss German University

Risk Management Analysis on Implementation of Information System in Organization Liantimoroan Using COBIT 5

Abrao Ximenes

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received: 1 December 2018
Accepted: 2 February 2019
Published: 25 April 2019
DOI: 10.33555/ejaict.v6i1.62

Corresponding Author:

Abrao Ximenes
Email: abrao.ximenes@student.sgu.ac.id

ISSN 2355-1771

ABSTRACT

Risk management analysis is to know about the implementation of information system, a part of risk management to be held within the organization to formulate a series of recommendation for the company. In order to get the final result in the form of documentation to support the further development of the system that will be described using COBIT 5 Framework, with the input of information technology processes that are running now. Then it will be obtained the maturity level, after it carry out an analysis of the maturity level has been obtained. The result of the analysis in the form of recommendation, as well as the methods that used to achieve the proposed recommendations.

Keywords: *Analysis Risk, Risk Management, Implementation Information System, Cobit 5*

1. Introduction

The continued development and progress of information technology in nowadays, it affects all aspects of human life. All aspects that ranging from education, business, government and others. At the beginning of the 90's implementation of computerization is still a rare thing that developed in many sectors due to very high cost and low operational cost benefits, but in the new millennium has begun the implementation of a computerized system applied to many areas and growing rapidly. Various systems developed using computer media and supporters and it makes most sectors started to develop information systems in business processes are implemented. Together with the development of information systems today are many scientific theories about utilization, management and other theories.

One aspect that is more important for the information system and its development is the aspect of security and risk management. Along with development of information systems nowadays some important things to be the deciding factor for the system that is running can function properly, because in addition to the positive effects arising from the development of the information system security issues and management of IT resources also occur. The institutions that depend largely on the business processes of information systems will experience serious problems when the system is not running properly applied. In this paper will conduct a study of risk management analysis on the implementation of information systems security in using a method ISACA is COBIT 5 (ISACA, 2012).

2. Framework

The Control Objectives for Information and Related Technology (COBIT) provide clear policies and good practices in the governance of technology to assist the management in understanding and managing the risks associated with information technology governance by providing a framework for information technology governance and guidance purposes detailed control objective for the management, business process owners, users and auditors. To make successful in delivering information technology needs the company's business, management must make the internal control system or framework. COBIT framework contributes to these needs with the control (Von Solms, 2005).

- Creating the relation with the company's business needs
- Organizing the information technology activities into a generally accepted process
- Identifying the major information technology resources that should be calculated
- Determining the control objectives management

The focus of COBIT is illustrated by a process model that divides information technology into 4 sections and 34 process that summarizes 210 detailed control objectives in accordance with their areas of responsibility, from planning, building, running and monitor the implementation of information technology, and also provide a view end-to-end information technology.

3. Information System Security

Systems that prevent fraud or at least detecting fraud in an information-based system, where the information itself has no physical meaning (Dhillon and Backhouse, 2000).

Threats

- The threats for information security always come from individuals, organizations, mechanisms, or events that have the potential to cause damage to the sources of companies' information.
- In fact, the threat may be internal, originating from within the company and externally or from outside the company. Threats can also occur intentionally or unintentionally.
- The insider threats come from the permanent employees, temporary employees, consultants, contractors, and business partners of the company.
- "SANS 2015 Survey on Insider Threats that was sponsored by SpectorSoft and conducted by the SANS Institute between December 2014 and January 2015. 772 IT security professionals regarding their experiences preventing and detecting insider threats within their organizations. Almost three-fourths of respondents (74 percent) are concerned primarily with employees, whether malicious or merely negligent, 44 percent of respondents said they don't know how much they currently spend on solutions that mitigate insider threats and 45 percent don't know how much they plan to spend on insider threat technology in the next 12 months "
- Insider threats is more serious danger than from outside the company, due to internal group has more knowledge about the system within the company.
- Countermeasures for outside threats are just starting to work if the attacks against security detected
- Countermeasures for the insider threats made to predict the security problems that might occur (Stoneburner, Goguen, and Feringa, 2002).

4. Methodologies

4.1 Literature Study

The literature study by collecting some theories, methods and models in the field of information systems management or Information technology in general, and also the governance of information technology in particular. Theories, methods and models is a method that is widely used and become a reference in academic, industry and practitioners of information technology in general.

The goal of the literature itself is:

- To be able to see an overview of the methods and frameworks used within the scope of information technology governance.
- Comparing the existing frameworks by identifying patterns and seek equivalence within this framework that will serve as a tool for assessing the management of enterprise information technology investments.

4.2 Data Collection

In this paper the data collection from primary and secondary data (Myers, 1997).

4.2.1 Primary data is data taken directly from the respondents obtained from:

Questionnaire: The data collection with this questionnaire is addressed to the IT staff at Liantimoroan made with a view to obtaining the target achievement and assessment of the achievements that have been implemented.

- Interviews: The collection data with this manner is done in order to determine the process and the steps being taken now associated with the management of information technology resources, decision making process, the process of managing information technology investment and also expectations of an ideal based on their views, as well as determining the factors should be considered at the time of investment in information technology will be conducted. The interview has down through Skype.

Secondary data is the data obtained from some of the reports that have been published by the company internally or particular institutions and maintained its validity.

5. Result of Risk Management Control

5.1 Result of Risk Management Per Domain (Primer)

The results of control evaluations of Risk Management per Domain is working to determine how much the maturity level of IT support processes primer per Domain (Sallé, 2004).

5.1.1 Plan and Organize (PO)

Tables 1. Result of Risk Management Control Domain (PO).

Number	Process	Number of Questions	Number of Values	Averages
1	PO 4	6	19	3.2
2	PO 6	6	20	3.3
3	PO 9	6	20	3.3

Number of Process: 3, Number of Averages: 9.8

Averages: 3.3

The table above indicates that the value of the Domain PO on the primary support is 3.3, this is a good value for a company in which existing procedures and implemented.

5.1.2. Delivery and Support (DS)

Tables 2. Result of Risk Management Control Domain (DS).

Number	Process	Number of Questions	Number of Values	Averages
1	DS 2	6	6	1.0
2	DS 4	6	16	2.7
3	DS 4	6	16	2.7
4	DS 11	6	17	2.8
5	DS 12	6	20	3.3

Number of Process: 5, Number of Average: 12.5

Average: 2.5

The table above indicates that the DS Domain value on the primary support is 2.5, this is a pretty good value for a company in which existing procedures, but has not been fully implemented

5.1.3 Monitoring and Evaluation (ME)

Tables 3. Result of Risk Management Control Domain (ME).

Number	Process	Number of Questions	Number of Values	Averages
1	ME 2	6	24	4.0
2	ME 3	6	23	3.8
3	ME 4	6	22	3.7

Number of Process: 3, Number of Averages : 12

Average: 4.0

The table above indicates that the value of the Domain ME in process primary support is 4.0, this is the ideal value of a company in which existing procedures, and has been implemented as well as the supervision of the management.

5.2 Result of Risk Management Per Domain (Secondary)

The results of Risk control evaluation is the level of process maturity value IT support per Domain. The management per Domain secondary function is to determine how the maturity value per domain.

5.2.1 Plan and Organize (PO)

Table 4. The result of Risk Management Control Domain (PO)

Number	Process	Number of Questions	Number of Values	Average
1	PO 1	6	21	3.5
2	PO 2	6	10	1.7
3	PO 3	6	12	2.0
4	PO 7	6	17	2.8
5	PO 8	6	12	2.0
6	PO 9	6	18	3.0

Number process: 5, Number average: 15

Average: 3.0

The table above indicates that the value of Domain PO on the secondary support is 3. Means it is a good value for a company in which existing procedures and implemented.

5.2.2 Acquire and Implement (AI)

Table 5. The result of Risk Management Control Domain (AI).

Number	Process	Number of Questions	Number of Values	Averages
1	AI 1	6	19	3.2
2	AI 2	6	18	3.0
3	AI 3	6	15	2.5
4	AI 4	6	16	2.7

Number of Process: 4, Number of Average: 11,4

Average: 2.8

The table above indicates that the value of Domain AI on the secondary support is 2,8. Means it is a good value for a company in which existing procedures and implemented.

5.2.3 Delivery and Support (DS)

Table 6. The result of Risk Management Control Domain (DS).

Number	Process	Number of Questions	Number of Values	Averages
1	DS 3	6	19	3.2
2	DS 7	6	17	2.8
3	DS 9	6	19	3.2
4	DS 10	6	17	2.8

Number of Process: 4, Number of average: 12.0

Average: 3 .0

The table above indicates that the value of Domain DS on the secondary support is 3,0. Means it is a good value for a company in which existing procedures and implemented.

5.2.4 Monitoring and Evaluation (ME)

Table 7. The result of Risk Management Control Domain (ME).

Number	Process	Number of Questions	Number of values	Averages
1	ME 1	6	20	3.3
2	ME2	6	18	3.0

Number of Process: 2, Number of average: 6.3

Average: 3.15

The table above indicates that the value of Domain Monitoring and Evaluation on the secondary support is 3,15. Means that it is a good value for a company in which existing procedures and implemented.

6. Conclusion

Based on the description and discussion in each of the previous chapter, it can be some conclusions as follows:

1. The conditions on the implementation of risk management information system security is good, this is evidenced by the value derived from IT support process as a whole is 2.8, which at this level already exists and implemented procedures.
2. The results of the evaluation of risk management controls per domain (secondary) is showed that the PO value average is 3.0, AI is 2.8, DS is 3.0 and ME is 3.15
3. The implementation should be done regularly to avoid mistakes in decision-making, data losing, computer operating errors and others.

References

Dhillon,.G., & Backhouse. J. (2000). Technical opinion: Information system security management in the new millennium, *Commun. ACM*, 43(7), pp. 125–128,

ISACA, (2012). A Business Framework for the Governance and Management of Enterprise IT, *Roll. Meadows ISACA.*

Myers M. D., et al. (1997). Qualitative research in information systems, *Manag. Inf. Syst. Q.*, 21, pp. 241–242.

Sallé M., (2004.) IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing, *Hewlett-Packard Co.* pp. 8–17.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Comput. Secur.*, 24(2), pp. 99–104,