Advances in Intelligent Systems Research, volume 172
Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)

Security Capability Assessment on Network Monitoring Information System Using COBIT 5 for Information Security

Aris PRATIWI[1], Dwi Rosa INDAH[2*], Jaidan JAUHARI[3]

and Mgs. Afriyan FIRDAUS[4]

[1,2,3,4]*Department of Information Systems Faculty of Computer Science Universitas Sriwijaya, South Sumatera, Indonesia*
**Corresponding author: indah812@unsri.ac.id*

ABSTRACT
PT Telekomunikasi Indonesia, Tbk. (Telkom) is a State-Owned Enterprises (SOEs), which provides products and services of information and communication technology services and telecommunications networks in Indonesia. Telkom has implemented a network disturbance monitoring information system which includes the NOSSA application. To ensure a reliable and safe system, it is necessary to measure the system's security capability. COBIT 5 for Information Security is a framework that can provide overall technical and non-technical information security governance. The results of the measurement for process EDM03, APO13, and DSS05 is at level 4 (processes that are running can be predicted), the process APO12 and BAI06 are at level 3 (the running process is stable). The capability of the measurement results can be used to recommend solving and decision making in the organization.
Keywords: *COBIT 5, Process Assessment Model, security capability assessment, network monitoring information system, information security*

INTRODUCTION

In the era of information and communication technology, information security becomes very important. Information security has become a fundamental issue for businesses, organizations, and governments while vulnerability Information Exchange Environment (IEE) has increased as the threat of widespread and complicated [1]. Information system security illustrates the protection of computer devices, data, facilities, and information from irresponsible parties, but in practice, information system security does not receive special attention from the system manager [2].
PT Telekomunikasi Indonesia, TBK (Telkom) is a State-Owned Enterprises (SOEs), which provides products and services of information and communication technology services and telecommunications networks in Indonesia [3]. To enhance the company's business needs Telkom has implemented the system for monitoring information system network interference, in which there are NOSSA applications (New Operation Support System Assurance). As one of the SOE, the company must implement an information security management system, it is relevant to the regulation of the Minister of Communication and Information about the information security management system implementation for the organization of the electronic system for public services [4].
Based on interviews and data recorded in 2017, the number of networks connected to Telkom's South Sumatra Communication Area (WITEL) is approximately 101 FIMO (Fiber Modernization) and 674 BTS (Base Transceiver Station) towers and has 178 million cellular subscribers. To ensure the system is reliable and secure, as providers of public services, Telkom is required to conduct an audit of the system, it is done to prevent loss of data and information that could be threaten for Telkom's operation activities [4].
One of the efforts to prevent this is the need for measurement of system security capabilities to determine the confidentiality, integrity, and availability because the system can be said to be safe if it meets these three principles. A framework that can provide comprehensive information security governance that specifically addresses security audits is called COBIT 5 for Information Security. COBIT 5 for Information Security can help companies to reduce their risks by managing security appropriately [5]. Information and related technologies are the core of the company, but information security is the core of stakeholder trust [6].

METHODOLOGY

The methodology of this study are as follows:

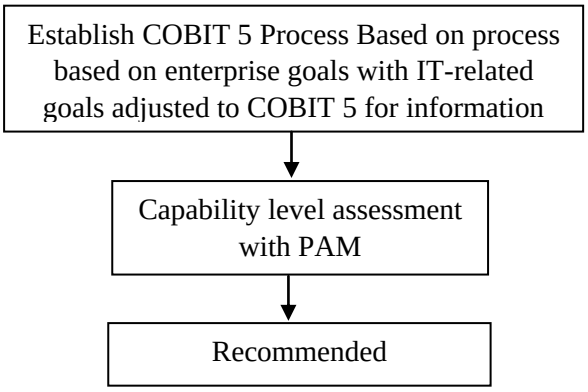

Figure 1 Research Framework

Based on Figure 1, the research framework starts from determining the COBIT process based on enterprise goals with IT-related goals adjusted to COBIT 5 for information security.
The next stage spread questionnaire to the respondents, the questionnaire responses are measured and analyzed using PAM (Process Assessment Model). The measurement results are analyzed and then make a recommendation to the optimization of the system, recommendations for improvement made by the interpretation of each level of process capability-based framework COBIT5. a measure of information system security capabilities and provides recommendations for improvements to improve information system security [7]

RESULTS AND DISCUSSION

Establish COBIT 5 Process

Table 1 shows the identification of enterprise goals. This mapping aims to reduce and formulate the objectives of the organization in the form of generic IT companies and related companies. Enterprise Goals following that defined by the COBIT 5 for Information Security framework [2].

Table 1. Identification of Enterprise Goal (EG)

BSC	Number	Y/T	Enterprise Goals	IT-Releted Goal (strategic plan)
Customer	EG-07	Y	Business service continuity and availability	Improved IT services Indi home Suggested Package (ISP)
Internal Business	EG-15	Y	Compliance with inter policies.	Improved information security with Sarbanes-Oxley Act (SOA).

Table 2. Result Mapping Enterprise to IT Related Goals

IT-Releted Goal (ITRG)	Enterprise Goals (EG)	
	EG-07 Business service continuity and availability	EG-15 Compliance with internal policies
IT-RG-7 Delivery of IT services in line with business requirements	S	
IT-RG-10 Security of information, processing infrastructure and applications	P	P

The results of the mapping between enterprise goals and IT-related goals are ITRG 10. Then ITRG 10 is mapped with the COBIT 5 process. The selection of COBIT 5 process is adjusted by considering the situation or circumstances in the enterprise[8]. The results of mapping are five processes obtained from primary categorized processes shown in table 3.

Table 3. Result mapping ITRG 10 COBIT 5 for information security

Domain	Process	COBIT 5 Process Name	ITRG 10- Information Security, processing infrastructure and applications
Evaluate, Direct and Monitoring	EDM03	Ensuring Risk Optimization	P
Align, Plan and Organise	APO12	Managing Risk	P
	APO13	Manage Security	P
Build, Acquire and Implement	BAI06	Manage Changes	P
Deliver, Service and Support	DSS05	Manage Security Services	P

Calculations Based Process Assessment Model (PAM)

From the questionnaire, obtained the answers as the number of questionnaires distributed to the respondents who had been mapped using RACI Chart. The results of respondents' answers are then made recapitulation outlines

$$Capability\ level\ index = \frac{\Sigma(answer\ x\ weight)}{\Sigma question} = \ldots\% \quad (1)$$

that can provide a picture inclination a level of capability on some attribute [9].

Process Assessment Model consists of dimensions and dimensional process that is used to assess the ability of the process capability levels. Capability is obtained by calculating each of the answers given by the respondents multiplied by weighting each answer has been determined and then divided by the total questions. The formula for computing the value of capabilities with the following formula [4].

Results level security capabilities of the network monitoring information system of the entire process shown in Table 4.

Table 4. Results Capability Level Security Systems

Process ID	Process Name	Process Assessment (%)									
		Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
			PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
EDM03	Ensuring Risk Optimization	FALSE	100	93.5	90.3	89.2	91	84.4	81.5	-	-
			F	F	F	F	F	L	L	-	-
	Level Capability							**Level 4 Predictable**			
APO12	Managing Risk	FALSE	100	91	86.5	87.6	82	-	-	-	-
			F	F	F	F	L	-	-	-	-
	Level Capability					**Level 3 Established**					
APO13	Manage Security	FALSE	100	94.8	92.3	93.8	92.2	85.7	83	-	-
			F	F	F	F	F	F	L	-	-
	Level Capability							**Level 4 Predictable**			
BAI06	Manage Changes	FALSE	100	87.4	89.5	88.3	83.3	-	-	-	-
			F	F	F	F	L	-	-	-	-
	Level Capability					**Level 3 Established**					
DSS05	Manage Security Services	FALSE	100	87.4	89.5	88.3	83.3				
			F	F	F	F	L				
	Level Capability					**Level 3 Established**					

The capability level of process manage risk and manage changes is at level 3 (Established) which means that the process that has been built is implemented, using a process that has been defined to achieve the expected results.
It shows that the company has been able to measure the extent to which the process of measuring the standard process is managed to support the execution of processes that have been defined and the company has been able to measure the extent to which the standard process is effectively run as it has been defined to achieve the results of the process.
The capability level to process ensure risk optimization, manage changes, manage security is at level 4 (predictable) which means predictable process. Processes that have run then operated with limits set to achieve outcomes expected from the security management process. shows that companies have to know how far the measurement results can be used to ensure that the performance of the process supports the achievement of organizational goals and processes assessed produce a stable process, capable, and predictable within limits defined.

Recommended Improvements

Recommendations for improvements in resume capability level conditions on the enterprise information system security as well as factors that should be fixed for each of the processes [10]. Recommendations made by the interpretation of each level of process capability-based framework COBIT 5.

Recommended Improvements for EDM03 Process

The following are recommendations for increasing the level of the EDM03 process (Ensuring Risk Optimization):

a. Check and assess continuously once every three months about the effect of risk on the current use of IT in the company.
b. Companies form his team for risk management and division of tasks and responsibility under the description of ISACA.
c. Always monitor the risk profile of corporate information so that the business risks and opportunities become balance.
d. Do not accept bug reports via chat or receive reports outside the application because it will have an impact on the integrity of the data.

Recommended Improvements for APO12 Process

Here are some recommendations to improve the level of the APO12 process (Managing Risk):

a. Identifying and collecting relevant data to identify, measure, analyze and report IT-related risks effectively.
b. Developing useful information to support the decision about risk contained in the relevant business risk factors.
c. Maintaining inventory of known risks and their attributes (including frequency expected, the potential impacts and responses) as well as related resources, capability, and control activities.

Recommended Improvements for APO13 Process

Here are some recommendations to improve the level of the APO13 process (Managing Security):

a. Conduct a review or assessment about the effectiveness of the ISMS (Information Security Management System) regularly (once in three months) to ensure that safeguards remain on the scope of the set and to record actions or events that could have an impact on the effectiveness of the performance for the network monitoring system.
b. Use application-proxy firewalls to filter information passed from the proxy server. Proxy servers can choose which information will be passed or not based on settings or logic from the proxy server.
c. Do not use the floppy drive to the server to avoid the intruder who can compose the root password using diskettes boot.
d. Provides UPS (Uninterruptible Power Supply) to the application or database server to prevent physical damage to the server.

Recommended Improvements for BAI06 Process

Here are some recommendations to improve the level of the BAI06 process (Managing Change):

a. Update documents and procedures whenever changes are implemented so that users affected by the change can adapt more easily.
b. Manage the day-care emergency changes to minimize further incidents and make sure these changes are controlled and proceeded securely. Ensure that emergency changes are measured and validated right after the changes.
c. Maintain tracking and reporting system for denied changes document, communicate the status of the approved changes, on the process and complete process documents.

Recommended Improvements for DSS05 Process

Here are some recommendations to improve the level of the DSS05 process (Managing Security Service):

a. Do the penetration test periodically (once in three months).
b. Determine the authorization of the devices that may access the institution information and institution networks, which means screen to code device (codification recording and manufacturing systems screening).
c. Apply encryption of information (the process of securing information by making the information can not be read without special knowledge) and make the information classification at the time of delivery.

SUMMARY

Based on the results of the questionnaire calculation, security capability assessment on Network Monitoring Information System obtained that the EDM03 process (ensuring risk optimization) is at fourth level, the APO12 process (managing risk) is at third level, the APO13 process (managing security) is at fourth level, the BAI06 process (managing change) is at third level and the DSS05 process (managing security services) has reached the fourth level. It can be concluded that the system has good security management.

To improve the capability level of the system process, there are some general recommendations for the whole processes that are:

a. Tighten control for the ongoing process so that it remains in a good position of security management.
b. The APO12 and BAI06 processes need to be implemented first to improve performance in business continuity, based on priorities.
c. Manage and evaluate the achievements consistently, especially control and evaluation every three months and every year.

REFERENCES

[1] Hassanzadeh, Mohammad, Narges Jahangiri, and Ben Brewster. "A conceptual framework for information security awareness, assessment, and training." Emerging Trends in ICT Security. Morgan Kaufmann, 2014. 99-110.

[2] Ramadhani, Surya Tri Atmaja, Rudy Hartanto, and Eko Nugroho. "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave Allegro Dan Kontrol Iso 27001 Pada Instansi Pelayanan Penyelenggara Publik." (2018).

[3] Telkom Profile (2018, November 11). Available in: www.telkom.co.id.

[4] Regulation of the Minister of Communication and Information of the Republic of Indonesia in 2017 concerning the Audit of the Implementation of Electronic Systems.

[5] Dimitriadis, C. And Stroud, R., , ISACA's Guide to COBIT 5 for Information Security

[6] Firdia, R. (2018). Information Systems Security Audit Article In the Bandar Lampung City Government Office Using COBIT 5.

[7] Dewi, C., Eko, N., & Adhipta, D. (2015). Information Systems Security Audit at Yogyakarta City Government Office Using COBIT 5. 66

[8] Indah, Dwi Rosa, Harlili Harlili, and Afriyan Firdaus. "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk." ICON-CSE 1.1 (2015): 113-117.

[9] Raja, GM, Suprapto, & Yusi, TM (2017, December 12). Governance Evaluation System Information Technology Security Framework Using COBIT 5 Process Focus APO13 and DSS05 (Study At PT Martina Berto). Development Journal of Information Technology and Computer Science, University of Brawijaya.

[10] Making of Information Security Management and IT Service Management Processes based on COBIT 5. Bandung.