Information Security For Hospital Information System Using Cobit 5 Framework

Khilda Nistrina
Faculty of Technology Management and Business
University Tun Hussein Onn Malaysia
8640 Parit Raja, Johor
Khildanistrina94@gmail.com

Prof. Dr. H. Abdul Talib Bin Bon
Faculty of Technology Management and Business
University Tun Hussein Onn Malaysia
8640 Parit Raja, Johor
talib@uthm.edu.my

Abstract

Background : Information security in Hospital Information System (HIS) become main issue in protected the patient privacy data due to it can be online accessed and susceptible attacked by malware- Misc-Activity. Therefore, the main objective of this study to investigate the capability level of information security in HIS. Method and Result: Quantitative method was performed in this study by questionnaire analysis in 86 respondents who apply HIS on the system. This study was conducted in selected hospital in Bandung, Indonesia which is Soreang Hospital and the information security in HIS was evaluated by COBIT 5. Evaluation results show that the capability level in the Soreang hospital is at level 1 for DSS05 domains with L (Largely achieved) criteria and level 0 domains for APO13 domains with L (Largely achieved) criteria. The improvement of information security in HIS required to achieve the expected Capability level which is fully achieved criteria.
Keywords : Information security, Hospital Information System, COBIT 5

1.0 Introduction

According to the Minister of Health issued the regulation No.89 in 2013 regarding Hospital Information System (HIS) aims to improve health services in Indonesia. That regulation stated that all hospitals are required to apply HIS and Emergency Respond Plan (ERP) system for improving healthcare (RI, 2011). HIS is one of the most common computer systems designed to support healthcare services (Bakshi & M, 2012). HIS are described as a complicated type, those systems have to support activities in hospital within application, tactical, and strategic levels (Pasandideh & Shafiri, 2016).

Nowadays, online system of HIS have many benefits for accessing patient record and transaction related to diagnosis patients. However, private data of patient become a serious issues due to it can be online accessed (Rai & Srivastava, 2014). Therefore, HIS required to equipped by information security that work with three basic aspects which called by protecting patient's data confidentiality, ensuring data integrity and assuring data availability. Improving the information security in HIS become a critical issues in the operation of information systems where the data that is stored and processed is particularly sensitive (Hou, Gao, & Nicholson, 2018). Although many efforts have been made to prevent information security threats, especially in the healthcare area, there are still many unknown risks which may threat the security of health information.

In HIS used many types of frameworks that focus on information security, but COBIT 5 framework is an appropriate frameworks for healthcare services due to it can be applied in any company and organization with any size (Luis Velez Lapao, 2012). Generally, COBIT has four domain and organization can consider using full COBIT framework, or organization can adopt specific control which the organization needs (Wolden, Valverde, & Talla, 2015). According to ISACA (2014), COBIT 5 has some process reference model and each process has different functions to ensure the users obtain the required data. Process reference model was divided in terms of field such as for outsourcing recommended using APO09 and APO10, for security using APO13 and DSS05, for software or hardware development

by BAI02, BAI03, BAI06, BAI07, and BAI10, for data center by DSS01 and for help desk by DSS02 and DSS03. According to Omari et al. (2012) stated, APO and DSS domain developments have the constraints both of time, resources, and implementing an audit framework of COBIT entirely is often considered as a large task. As an alternative to reduce the size of COBIT 5 framework for the public sector can use some domain control from the framework.

The most common threats to the information security are unauthorized use of software and computers for communications and illegal activities (Ayatollahi & Shagerdi, 2017). Based on the monitoring of internet traffic carried out by the highest attack in Indonesia Security Incident Response Team on Internet Infrastructure in 2017, almost reached 32,081,950 million malware- Misc-Activity is active in internet traffic, this indicates that the vulnerability of the system is connected to the internet there is a big chance of being known for malware, which led to system damage and even changes and corrupted data [9]. Based on the report that issued by the Minister of Communication and Information, Rudiantara [10], stated that the awareness of the Indonesian people towards cyber is still very low. Referring to the data released by Global Cyber Security Index (GCI) in 2017, Indonesia is ranked 70th from 195 countries for cyber security. According to [11] Indonesia is among the top 10 countries that have been hit by attacks at any time. For example, one of the incident at a hospital in Indonesia as reported by (Yusuf, 2017), a ransomwarewannacry (another name wannadecryptor) began to be detected on 12 May 2017. Wannadecryptor starting to attack a lot of companies and one of them is hospital software system. In order to recovery the data, they need to pay for it. Another issue is misuses of data and data lost, because HIS has been integrated of several systems in the hospital to manage administration works, patients and clinic records (Ramdas & Ankitha K, 2017).

From the related issues above, this research was focused on evaluation information security of hospital information system by COBIT 5 framework. This research aims to examine the capability level of Hospital Information System in term of information security and to identify the strengths, weaknesses, and risk of a particular process, so that can be seen whether the process is moving toward a defined goal or not and ultimately it is hoped that the improving quality of healthcare services.

2.0 Method

The research was conducted on selected government hospital in Bandung, Indonesia which is Soreang Hospital. The monitoring activity was performed from June to August 2018. This research was carried out using quantitative method, which include questionnaires the survey guided by COBIT 5 Capability level is looking at the activity points in each domain to determine the level of capability of each domain such as DSS05 and APO13. Questionnaires for the DSS05 domain have questions related to minimizing the business impact that will occur from the vulnerability in the operation of information security and in accordance with the capability level. Meanwhile, for APO13 consists of the question in terms of establishing and maintaining information security management systems, define and managing information security risk treatment plans, monitors, and review the information security management system. The questionnaire will be divided into several agreement levels as listed in Table 1. This study involve 86 respondents who consists of staffs at hospital who apply HIS on the system. The quantitative analysis will be selected using purposing sampling, based on the assumption that the researcher want to investigate and understand an issue based on several samples (Ismail, Abdullah, Shamsudin, & Ariffin, 2013).

Table (1). Agreement level

Score	Category
1	Strongly disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly agree

3.0 Result

The capability level of DSS05 domain for HIS in Soreang hospital based on COBIT 5 Framework for information security is listed in Table 2. The results shows that from 86 respondents, 31,4% were male and 68,6% were female. In terms of education level of respondents, 36% of respondents were at education levels of diploma, 36% had bachelor's degree, 3,6% were graduated with master's and 25% were high school diploma or lower. In addition, the age of respondents were consists of 52.3% of respondents in between 21 and 30 years old, 37.2% in between 31 and 40 years old, and 10.5% of the respondents in older than 41.

The capability level also investigated in different workplace such as 25.6% of respondents working at pharmacy installation, 13.9% of respondents working at laboratory installation, and 60.5% of respondents working at administration and management. Based on the results shows that the capability level of respondents for each process can be calculated.

Table (2). Capability level of DSS05 domain for HIS in Soreang hospital based on COBIT 5 Framework for information security

Process Name	DSS05									
Purpose	Minimize the business impact of operational information security vulnerabilities and incidents									
Level	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
Process atribut		P.A 1.1	P.A 2.1	P.A 2.2	P.A 3.1	P.A 3.2	P.A 4.1	P.A 4.2	P.A 5.1	P.A 5.2
Rating by percentage (%)	85.1	72.5	70	71.2	73.8	69.5	73.2	71.5	71.8	70
Rating by Criteria	F	L	L	L	L	L	L	L	L	L

Note: F is fully achieved and L is largely achieved

From Table 2 shows that for level 0 on DSS05 has reached of 85.1% or F (Fully achieved) which means that the achievement process already has complete and systematic evidence for, and full achievement of, the attributes that have been determined in the process being assessed. In this level have not a significant weaknesses related to this attribute in the assessment process. While for level 1 to level 5 in DSS05, it is at L (Largely achieved) criteria which means that the achievement process already has evidence of a systematic approach to and significant achievement of the attributes that have been determined in the process being assessed. The process that is considered may have several weaknesses associated with this attribute. The capability level obtained for the DSS05 domain is level 1 with largely achieved criteria. In accordance with the theory of capability level, fully achieved criteria when the level reach 85% - 100% and it can proceed to the next level. However, largely achieved criteria obtained when the level below than 85% then it cannot proceed to the next level (ISACA, 2014).

Evaluation details of poses managing services at level 1 are: the first is for protect against malware, the hospital has been implemented and maintained an existing processing facilities install and activate malicious software protection tools, anti-virus is always updated automatically or semi-automatically. The second is manage network and connectivity security, the hospital network filtering has been implemented to control incoming and outgoing traffic.The third is Manage endpoint security,the hospital has been managing endpoint of the use of information such as laptops, desktops, server or other software.The forth is manage user identity and logical access, the user accessin accordance with their business function and process requirements. The fifth is manage physical access to IT assets, the hospital has been recorded and monitored access to the building, this must be done to all persons entering the building, including staff, temporary staff, clients, vendors, visitors, and others. The sixth is manage sensitive documents and output devices, the hospital has been protecting sensitive information. And the last is monitor the infrastructure for security-related events, the hospital has been monitored the infrastructure in unauthorized access. Moreover, the capability level of APO13 domain for HIS in Soreang hospital is listed in Table 3.

Table (3). Capability level of APO13 domain for HIS in Soreang hospital based on COBIT 5 Framework for information security

Process Name	APO13									
purpose	Keep the impact and occurrence of information security incidents within the enterprise risk appetite levels									
Level	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
Process atribut		P.A 1.1	P.A 2.1	P.A 2.2	P.A 3.1	P.A 3.2	P.A 4.1	P.A 4.2	P.A 5.1	P.A 5.2
Rating by persentage (%)	68.2	66.6	73	69.5	72.7	69.4	66.8	72.5	74.8	67.6
Rating by Criteria	L	L	L	L	L	L	L	L	L	L

From Table 3 shows that for level 0-5 in APO13 has rating of 68.2-74.8% which include in the Largely achieved criteria, which means that the achievement process already has evidence of a systematic approach to and significant achievement of the attributes that have been determined in the process being assessed. The process that is considered may have several weaknesses associated with this attribute. Assessment details of poses managing services at level 0, is: The hospital is little or no evidence of any achievement of the process purpose.

4.0 Conclusions

The capability level of HIS for DSS5 and APO13 has been analyzed and the rating of the levels majority in L criteria. The information security for DSS5 domain for level 1-5 was in largely achieved status of 70-73.2%.While, level 0 was in F criteria with rating value of 85.1%. In addition, for APO13 domain for level 0-5 was in largely achieved status of 68.2-74.8%. Therefore, the information security in Soreang hospital require to improved due to several weaknesses associated with this attribute. Some recommendation of to improve HIS has been formulated such as the first recommendation is for DSS05 namely Improve a standard procedure for hardware management operations to protect computers from malware threats such as viruses, worms, spam, and others. Making governance policy regulations and right internet usage. Management using passwords (scheduling for password change rottenly) and establish operating system procedures regarding the data back-up process regularly and periodically in order to avoid data loss, data theft, data tapping, data destruction by irresponsible people and IT threats or interruptions. The second recommendation is for APO13 namely Identify members involved in information security management activities in HIS, identify roles and responsibilities in detail in order to know the members responsible for monitoring, evaluating, and assessing the running system performance and Improve a standard procedure for security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.

References

Aksu, P. k., Kitapci, N. S., Catar, R. O., Koksal, L., & Mumcu, G. (2015). An Evaluation of Information Security from the Users' Perspective in Turkey. *Journal of Health Information in Developing Countries*, 55-67.

Arcidiacono, G., & Nuzzi, S. (2017). A review of the fundamentals on process capability, process performance, and process sigma, and a introduction to process sigma split. *International journal of applied engineering research*, 4556-4570.

Ayatollahi, H., & Shagerdi, G. (2017). Information security risk assessment in hospitals. *The open medical informatics journal*, 37-43.

Ayuwuragil, K. (2017, 12 6). *Kesadaran keamanan siber Indonesia peringkat ke-70 dunia*. Diambil kembali dari www.cnnindonesia.com: https://www.cnnindonesia.com/teknologi/20171206162248-185-260555/kesadaran-keamanan-siber-indonesia-peringkat-ke-70-dunia

Bakshi, S. M., & M, S. (2012). A study on Hospital Information System at a Tertiary Teaching Hospital. *Global journal of cumputer science and technology interdisciplinary*.

Erdianto, K. (2017, 11 21). *Keamanan siber Indonesia tak lebih baik dibandingkan Malaysia dan Singapura*. Diambil kembali dari www.nasional.kompas.com: https://nasional.kompas.com/read/2017/11/21/20480051/keamanan-siber-indonesia-tak-lebih-baik-dibandingkan-malaysia-dan-singapura

Hou, Y., Gao, P., & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *ScienceDirect*, 64-75.

ID-SIRTII/CC. (2018, 10 22). *Data Internet Trafik Tahun 2017.* Diambil kembali dari www.idsirtii.or.id: https://idsirtii.or.id/trafik/tahunan/2017.html

ISACA. (2014). *Basic Foundational Concepts Students Book: Using COBIT 5.* USA: ISACA.

Ismail, N. I., Abdullah, N., Shamsudin, A., & Ariffin, N. (2013). Implementation differences of hospital information system (HIS) in Malaysian public hospitals. *International journal of social and humanity*, 115-120.

Luis Velez Lapao, M. P. (2012). Organizational challenges and barriers to implementing IT governance in a hospital. *journal information systems evaluation, 14*(1).

Pasandideh, R., & Shafiri, F. (2016). Evaluating hospital information system in selected hospitals of Tehran city according to ISO 9241-10 standard. *International academic institute for science and engineering*, 1-9.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals.* NISTIR.

Rai, B. K., & Srivastava, A. (2014). Security and privacy issues in healthcare information system. *International journal of emerging trends of technology in computer science (IJETTCS)*, 248-252.

Ramdas, S., & Ankitha K. (2017). Adviced protection for patient information in medical database. *international journal of computer science and mobile computing*, 478-488.

RI, K. K. (2011). *Kementerian KEsehatan Republik Indonesia*. Dipetik March 5, 2018, dari www.depkes.go.id: http://buk.depkes.go.id/index.php?option=com_content&view=article&id=224:pertemuan-koordinasi-teknis-it-dalam-rangka-e-health

Samy, G. N., Ahmad, R., & Ismail, Z. (2009). Threats to Health Information Security. *2009 Fifth International Conference on Information Assurance and Security*.

Sheikhpour, R., & Modiri, N. (2012). An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Control. *International Journal of Security and Its Applications*, 13-27.

Sligo, J., Gauld, R., Roberts, V., & Villa, L. (2017). A literature review for large-scale health information system project planning, implementation and evaluation. *ScienceDirect*, 86-97.

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal Of Conteporary Research In Business*, 329-254.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *sciencedirect*, 1846-1852.

Yusuf, O. (2017, May 13). *Rumah sakit di Jakarta disandera "Ransomware", minta tebusan Rp 4 Juta*. Dipetik March 18, 2018, dari Kompas: www.kompas.com

Biography / Biographies

Khilda Nistrina is an student master of technology management at the Universiti Tun Hussein Onn Malaysia, Johor, Malaysia. She was born on November 11, 1994, in Bandung, West Java, Indonesia. Completed primary School in Bandung, West Java, Indonesia in 2006. Completed junior high school at SMPN 1 Baleendah, Bandung, West Java, Indonesia in 2009. Senior high school in SMAN 1 Baleendah, Bandung, West Java, Indonesia in 2012. She earned degree in Computer Science Cducation from Indonesia Education University, Bandung, Indonesia in 2016. She has taught courses in networking, algorithms, mathematics and chemistry for high school students.

Abdul Talib Bin Bon is an Professor of Production and Operations Management in the Faculty of Technology Management and Business at the Universiti Tun Hussein Onn Malaysia since 1999. He has a PhD in Computer science, which he obtained from the Universiti de La Rochelle, France in the year 2008. His doctoral thesis was on topic Process Quality improvement on Beltline Moulding Manufacturing. He studied Business Administration in the Universiti Kebangsaan Malaysia for which he was awarded the MBA in the year 1998. He's bachelor degree and diploma in Mechanical Engineering which his obtained from Universiti Teknologi Malaysia. He received his postgraduate certificate in Mechatronics and Robotics from carlisle, United Kingdom in 1997. He had publised more 150 International Proceedings and International Journals and 8 Books. He is a member of MSORSM, IIF, IEOM, IIE, INFORMS, TAM, and MIM.