(IJID) International Journal on Informatics for Development,
Vol. 3, No. 1, 2014

Hospital Information System Audit Using The ISO 27001 Standard

(Case Study In RSU PKU Muhammadiyah Bantul)

Heri Setiawan
Department of Informatics
Faculty of Science and Technology
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
erys999@gmail.com

Khurin 'ien Mukhoyyaroh
Department of Informatics
Faculty of Science and Technology
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
khurin.11a3.12@gmail.com

Muhammad Dzulfikar Fauzi
Department of Informatics
Faculty of Science and Technology
Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
dzulfikar1234567@gmail.com

Bambang Sugiantoro
Master of Informatics
Faculty of Science and Technology, Universitas Islam Negeri Sunan Kalijaga
Yogyakarta, Indonesia
bambang.sugiantoro@uin-suka.ac.id

***Abstract*—RSU PKU Muhammadiyah Bantul have been using information technology to improve health care in their area. One of the uses of information technology is in medical record information system. The existence of medical record information system will help to manage all medical record data. But with applying information system its data need to be secured, while there still less knowledge and understanding about medical record information system security. Therefore, it's needed to have an audit using the standard of ISO 27001 to get a convenient security service for a medical record information. The audit of ISO 27001 used because this standard focus at information system security and use as the national standard of Indonesia. This standard contains complete determination to discover information system security. This research managed to give an assessment for medical record information system security of RSU PKU Muhammadiyah Bantul with maturity value of 2,2 (Repeatable but Intuitive). So medical record information system security of RSU PKU Muhammadiyah Bantul is good enough because it's been followed the information system security procedure. But the hospital management is not paying attention regarding the understanding of their employees about information system security for their medical record information system.**

Keywords--Audit System; ISO 27001; Medical Record Information System

I. INTRODUCTION

One of the agencies that require the use of information system is the hospitals. The existence of a hospital information system will make it easier to manage all hospital data, such as medical records data, polyclinic data, laboratory data, pharmacy data and data from another unit in the hospital. To get a good hospital information system service, it is necessary to have good information system management, including the security management of the information system.

One of the method of managing information system security that is often used is ISO 27001 (International Standard Organization 27001) [1]. This standard helps organization to keep information assets secure [1].

II. PURPOSE

The formulation of the problem raised from the background above is:

1) Produces a hospital infomation system security assessment according to ISO 27001 standard.

2) Produce a recommendation for a good management of hospital information system security in accordance with ISO 27001 standards.

III. RESEARCH METHOD

A. Data Collection Methodology

Data were collected from various sources. Data collection methodology performed in this study are:

1) Literatur Study: Literature studies were conducted to obtain theories about information system security audits, regarding the same audit process and had been carried out by the previous research, also supporting theories for this research. Weber in [2] defines an audit of an information system is a process to collect and evaluate evidences to assess whether that information system could protect assest, and information technology that is used could maintain data integrity so the goal of business could be achieved effectively with available sources. In addition to theories relate to information system security audits, previous research relate to audit of information systems are also studied. Two of them are research by Kusuma [3] and Unggara [4].

2) Observation: Observation are made to determine the conditions of management and implementation of the running information system. In observation, communication was also maintained with the management side who is responsible for the governance and implementatiom of the hospital imformation system.

B. Identification Problem

The main problem that occurs is how to provide an assessment for the management of hospital information system security in accordance with ISO 27001 standard and how to recommend good management of hospital information system security according to ISO 27001 standards.

C. Problem Scope

1) This research uses ISO 27001 standard.

2) The object study is a hospital information system, named a medical record information system.

3) The basic of the security control area of ISO 27001 used are 3 targets, that is :

a) Asset management

b) Physical security and environment

c) Access control

IV. RESULT AND DISSCUSSION

A. Audit Process

In this audit, interview process will be conducted on:

1) Audit CEO

In the audit process, the auditor uses Form Question 1 (FQ 1). This form question 1 contains 51 question that are part of the Master Question (MQ) and the description of the clause on the master control. All questions will be asked to those who is responsible for information system at RSU PKU Muhammadiyah Bantul, during the audit process, the role of CEO was Anwar Siswati, S.Kom as head of EDP.

2) Infrastructure Admin Audit

In the audit process, the auditor uses Form Question 2 (FQ 2). This form question 2 contains 13 question that are part of the Master Question (MQ) and the description of the clause on the Master Control (MC). All questions will be asked to the infrastructure admin who is responsible for the management of hardware and network information system at RSU PKU Muhammadiyah Bantul. In this audit process, the role as infrastuctur admin was Karjono, S.Pd and Agus Siswanto, A.Md as staff of the EDP unit.

3) Software Admin Audit

In the audit process, the auditor uses Form Question 3 (FQ 2). This form question 3 contains 3 question that are part of the Master Question (MQ) and the description of the clause on the Master Control (MC). All questions will be asked to the admin software who is responsible for the management of information system application at RSU PKU Muhammadiyah Bantul. In this audit process, the role as admin of the software was Arie Hermanto, A.Md as the EDP unit staff.

4) Audit Operator

In the audit process, the auditor uses Form Question 4 (FQ 4). This form question 4 contains 31 question that are part of the Master Question (MQ) and the description of the clause on the Master Control (MC). All questions will be asked to the operator using the application of the medical record information system at RSU PKU Muhammadiyah Bantul. In this audit process, the role as opeator was Tri Murlinawati, A.Md and Kasturi, A.Md as the medical record unit staff.

B. Audit Result Analysis

The audit process uses Form Question 1 (FQ 1) audit paperwork for the CEO, Form Question 2 (FQ 2) for infrastructure admins, Form Question 3 for admin software, Form Question 4 (FQ4) for operators, then the maturity model data for each target control area has been obtained. The data is obtained from the average of all score of each question given during the interview.

TABLE I. THE RESULT OF THE TARGET AREA'S MATURITY MODEL

CLAUSE	CONTROL TARGET	TEST RESULT	MTURITY
A.7	Asset Management	Repredictable but intuitive	2,4
A.9	Physical and environmental security	Repredictable but intuitive	2,2
A.11	Access management	Repredictable but intuitive	2,01

1) Analysis of The Results of The Asset Management Audit

For the result of the audit on the asset management control target obtained a 2.4 maturity value, therefore asset management in the medical record information system at RSU PKU Muhammadiyah Bantul has implemented an asset management procedure followed by employees. But the management of RSU PKU Muhammadiyah Bantul has not provided formal training o asset management. In managing this asset RSU PKU Muhammadiyah Bantul is still lacking in checking assets that are not routine or periodic. To clarify the data accessed by the user is also not maximal because it is not in a rule or procedure at RSU PKU Muhammadiyah Bantul. However, the maturity value in this clause is close to 2.5, which means that the asset management process is not well documented and there is a mentoring process although it is done periodically. Therefore, RSU PKU Muhammadiyah Bantul is enough to increase routine checking of asset inventories and create procedures for classifying data and implementing it to improve security in asset management clauses.

2) Analysis of the results of audit physical and enviromental security

The results of the audit process on objectives of physical and environmental security control produce 2.2 maturity values.so that the physical and environmental security of the medical record information system of RSU PKU Muhammadiyah Bantul has followed the existing physical and environmental security procedure. But there is no formal training related to physical and environmental security that is given to related employees so that possibility of each other's mistakes may occur frequently. In this clause the arrangement of the medical record information system in the registration unit is not maximal because the user still feels uncomfortable, less extensive and the other unit employees too often pass. Users can still easily use the *flash disk* and *copy* hospital data, even though it is for hospital purposes but the possibility of data theft can still occur. Communication between the EDP head and EDP staff was not good because it was found by staff who were not sure of the *hardware* checking procedure.

3) Analysis of The Results of Access Control Audits

The target of access control produces a *maturity* value of 2.01 (*Repeatable but Intuitive*). So it was obtained that access control in the medical record information system of RSU PKU Muhammadiyah Bantul was good enough because it had followed existing access control procedures. There is already a division of access rights between leaders and staffs. Access control for internet use only for hospital need is still in the form of an appeal not yet in hospital rules or policies. Users have never changed passwords during work. Not all employees are given user ID and password independently, as evidenced by the existence of employees who use the medical record information system using the user id and password of their supervisor. Even though they have never accessed their supervisor's data, it is possible that this can still happen. Users also can still access social media with computers during working hours. Users still often leave the medical record information system without *logging out* even though no adverse events have occurred but it allows others to see data from the medical record information system. For security from outside parties, for example PKL students are still lacking because PKL students are given direct access to the medical record information system so that the possibility of PKL students doing data theft with *flash disks* can occur. EDP units need to increase network security because there is no written policy on network security. Checking the network if there is only damage, it is not routinely and periodically checked.

V. CONCLUSION

A. Audit Results

This research managed to give an assessment for medical record information system security of RSU PKU Muhammadiyah Bantul with maturity value of 2,2 (Repeatable but Intuitive).

B. Audit Recommendation

1) In the asset management control clause, it is necessary to check the asset inventory by the EDP team and the Procurement unit at least 3 (three) months.

2) In the physical and environmental security control clause, it is necessary to prohibit the use of flash disks on staff, data retrieval with a flash disk is only allowed for the head of the unit or assistant head of the unit. Spatial planning and information systems for medical records must be adjusted to the conditions of the room, for example 1 (one) computer for 1 (one) user at least 2 (two) meters away with the computer and other users.

3) In the access control clause, it is necessary to impose written rules regarding internet access usage during working hours, all employees who have a user id and password must change passwords regularly every 3 (three) months, every employee who uses a medical record information system must be given a user id and the password independently and may not use the user id and password of other employee or even the user id and password of his supervisor even though it is temporary, all external parties such as training students are not given access

to the medical record information system, if the training student helps the registration process, there are still employees who input data into the medical record information system, for the EDP team it is necessary to check the medical record information system application in all units using at least 2 (two) months.

REFERENCES

[1] Anonym, ISO/ IEC 27001 Information Security Management. Accessed from https://www.iso.org/isoiec-27001-information-security.html.

[2] Iffano, and Sarno, R., Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press, 2009.

[3] R. A. Kusuma, "Audit Keamanan Sistem Informasi dengan Menggunakan Standar SNI ISO 27001 pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta," UIN Sunan Kalijaga Yogyakarata, 2013.

[4] R. Unggara, "Audit Sistem E-Learning Fakultas Sains Dan Teknologi Uin Sunan Kalijaga Yogyakarta Menggunakan Framework Cobit 4.1," Universitas Islam Negeri Sunan Kalijaga Yogyakarta, 2013.