Evaluation and Recommendation IT Governance in Hospital Base on COBIT Framework

Johanes Fernandes Andry, James Surya, Christian Salim, Dela Haeraini

***Abstract*— RSAL Mintohardjo is a hospital which is engaged in services, and research. As one of the major hospitals with high complexity business processes, information system audit is required to evaluate the hospital IT service. This research will use one of the COBIT domains of Delivery and Support which will specifically focus on DS5, DS9 and DS10 process. The purpose of the IS audit on hospital is to find a weak point on the application of information systems by the hospital at this time and to evaluate whether to ensure the operational standard of the procedure can support the achievement of the hospital goal. From the results of this study it can be concluded that Domain DS obtained the maturity value of 3 from the expected level 4. It means that the overall hospital has realized the need for the MIS as well as standard procedures, formally documented, and already implemented.**

Keywords—Audit, Information System, COBIT 4.1, Delivery and Support.

I. Introduction

Information communication technology (ICT) and Information System (IS) has been a backbone of business and management in many years; its value investment has grown and increased [1]. Todays, many organizations and companies that have been implemented ICT/IS are becoming crucial role player for any organizations to achieved their goals [2], and become a champion in this global of market and competitive era [3]. Effectiveness and efficiency for IT Governance [4], helps and make sure that ICT/IS supports, helps management and business goals [5], optimizes and improved business investment in ICT, and appropriately management IT-related treat and opportunities [6]. IT governance (ITG) are a process by which the objectives of the entity that give impact on IT are agreed, directed, managed, measurable and controlled [7]. The primary goal of ITG is on the responsibility and control of the board of director and executive management to direct control and calculated formulation the implementation of ICT/IS strategy [8], to make sure the alignment of ICT and profit the business, and to identify metrics for calculated the management and business value of ICT and to manage IT risks in an to the right things way [9].

Enterprises or organizations understand the grow up importance of ICT/IS and consider it a treasure in enhanced their value competitive advantage position [10] and increasing value to their IT & business [11]. So, Information Technology used to provides cost and benefits at several levels of many companies, organizations, government and civil society [12].

Rumah Sakit Angkatan Laut (RSAL) or NAVAL Hospital Mintohardjo has implemented information systems, and planned to be implemented for the development of hospital information system. The expectation of the use of IT is in an effort to get the various facilities and benefits of IT, so it is expected to help the company's performance to conduct a competitive business strategy [13]. In this paper, the authors will conduct an analysis using the COBIT 4 framework. COBIT is a set of guidelines that are applicable and applied to support IT performance as well as corporate governance [14].

1.1 The Objective of the Study and Statement of the Problem

The paper investigated and audit of information systems, which sought to answer the following question (1) Is the application of information system on RSAL Mintohardjo in accordance with company procedures? (2) What is the level of information system maturity at Mintohardjo Hospital? (3) How to use the information system audit result for evaluation of hospital information system based on COBIT framework on Delivery and Support domain? The result of the study will be recognizing the improvements and made to recommend to Hospital.

The objective of the audit information system contained in RSAL Mintohardjo is to look for errors and deficiencies in information systems that are currently applied as well as to evaluate to ensure that the hospital needs for information systems are in accordance with operational standards procedures applied. Therefore the need for an audit information system to evaluate the system of the hospital. Purpose of the implementation of this system audit is to evaluate and make the results of the audit as input to improve the running system management at Hospital so as to realize the company's IT objectives is to have an integrated ERP for this service line of business. Audits conducted on companies on ITG ongoing data security [15].

1.2 The Significance of the Study

This research will use one of the COBIT domains of

J.F. Andry is Senior Lecturer in Department of Information Systems, Faculty of Technology and Design, University of Bunda Mulia, North Jakarta, 114430, Indonesia (e-mail: jandry@bundamulia.ac.id). James Surya[1], Christian Salim[2] and Dela Haeraini[3] are students in Department of Information Systems, Faculty of Technology and Design, University of Bunda Mulia (email: jamessuryaseputro@yahoo.com[1], christiansalim46@gmail.com[2], delahaeraini@gmail.com[3]).

Delivery and Support (DS) and will focus on DS5, DS9, and DS10. The selection of domains is tailored to the research focus encompassing the maintenance and protection of IT assets, ensuring the integrity of hardware and software configurations, identifying and classifying problems for improvement, and ensuring effective management of data.

II. Related Literature and Studies

A. COBIT

The information system audit serves to ensure the information system within the company safeguards information assets, uses the system effectively and efficiently and maintains integrity [16]. Audit is a collection process and evaluation of all information systems activities within the company are used to measure how far the system that has become a provision in the company has been running well [17]. Control Objective for Information and Related Technology (COBIT) is the information communication and technology governance standard, which applies to management and board, Information Technology provide services, to control department, to audit functions and processes, and more importantly the board and owners of the business and management process to make sure the detail, integrity, and availability of file, data and information which are most important and sensitive [18].

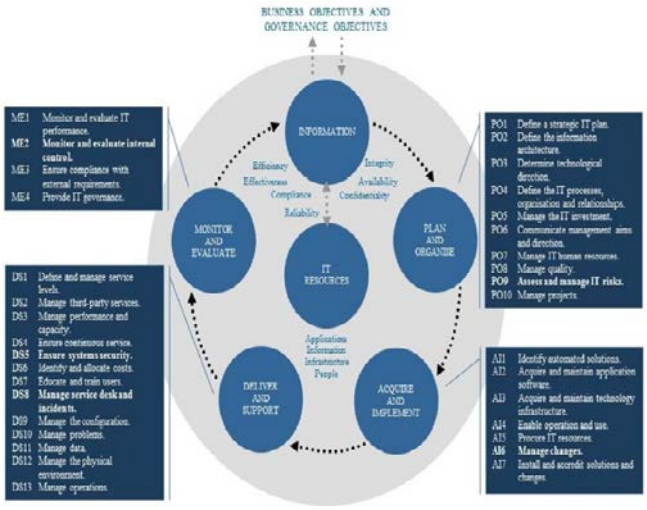

Figure 1. COBIT Framework [20]

Best practice of COBIT has been proved and to provide a successful standard for ICT governance in a controlled and measureable environment. In Fig. 1, COBIT Framework there are 4 (four) main domains under which there are 34 (thirty four) top ranking control objectives and goal listed below [19]:

a) Plan and Organize (PO),
b) Acquire and Implement (AI),
c) Deliver and Support (DS),
d) Monitor and Evaluate (ME).

Managers or leader at all levels domain in all functions to enable them to make timely and effective decisions for planning, directing and controlling the activities for which they are responsible [21]

B. Maturity Level

In COBIT 4.1 Maturity level management Information Systems and Information Technology (IS & IT) can be divided into 6 (six) levels, the sixth level specification can be seen on Table 1. Maturity Level of Hospital.

Table 1 Maturity Level of Hospital [17]

Level & Index	Description
Level 0 Nothing Index 0 - 0,49	The Hospital is not at all concerned about the importance of information technology to be managed well by management
Level 1 Initial/ Ad Hoc Index 0,50 - 1,49	The Hospital is reactively doing the application of information technology in accordance with immediate needs, without preceded by planning previous
Level 2 Repeatable But Intuitive Index 1,50 - 2,49	The Hospital already has a pattern repeatedly done in doing management of activities related to governance information technology, but its existence has not been well-defined so formally still inconsistent
Level 3 Defined Index 2,50 - 3,49	The Hospital already has the standard procedure formal and written communications to all stakeholders to be obeyed and done in daily activities
Level 4 Managed and Measureable Index 3,50 - 4,49	The Hospital already has a number of indicators which serve as each target Application of information technology applications.
Level 5 Optimized Index 4,50 – 5,00	The hospital has implemented governance manage the information Technology that it refers to "best practice".

III. Methods

In this study, the authors make observations and methods of direct interviews to parties directly related to application system.

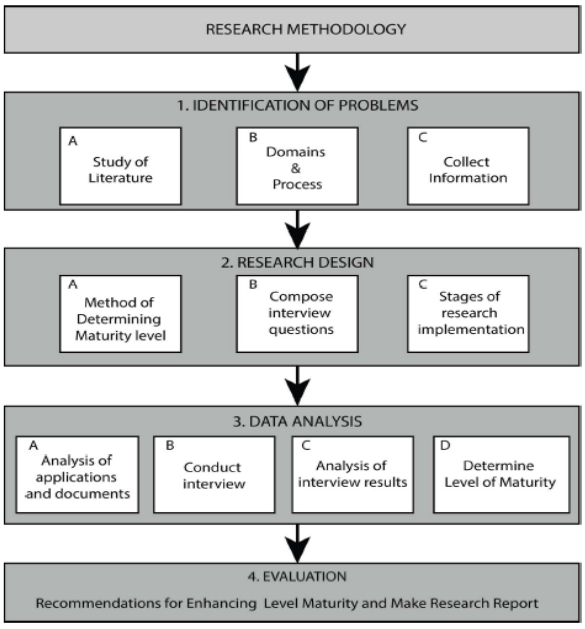

Fig. 2. Research Methodology [22].

Where this is done so that the results of this analysis really become an accurate result of the condition of the system used by employees in this company. This study uses the COBIT 4.1 framework to provide recommendations for the resulting level capabilities.

Methods of data collection to be used here are through interviews and from literature studies. This study focuses on Domain DSS and processes DS5, DS9 and DS10. DS5 is used because it aims to Ensure Systems Security in NAVAL Hospital. DS9 is used because it aims to manage the configuration by providing input, process and how to overcome them. DS10 is used because it aims to Manage Problem by identification and classification of problems, root problem analysis and problem solving. In this section the author will explain in connection with the existing research methodology which is divided into 4 parts, the method is illustrated in Fig. 2 Research Methodology.

3.1 Identification of problem (Case Study NAVAL Hospital)

a. The first step done by the author is to conduct a study of literature related to the purpose of doing this research.

b. Then the auditor will determine the domain to be used and also the process suitable for use based on existing sources after the next identification process will be done the appropriate domain selection from the existing domain in COBIT 4.1, especially domain DS5, DS9 and DS10.

c. The auditor will collect relevant information and will limit the scope of existing research.

3.2 Research Design

a. In the second stage is started with a description of the method that will be applied to determine the system level of Maturity.

b. Make a list of questions to be asked to the resource persons.

c. Stages to examine the implementation will be used.

Data Analysis

a. Conducting analysis of application system and document adjustment.

b. After the analysis and the document has been adequate then will be conducted interviews based on the domain that has been determined.

c. Conduct analysis of calculation of interview result.

d. Determine the level maturity based on the conversion result of interview analysis that has been done.

3.3 Evaluation

Provide recommendations to improve existing level maturity and form a report for the company to provide feedback on the results of research that has been done.

IV. Results and Analysis

In this section will be the discussion and explanation of the analysis conducted based on research methodology that has been run. Researchers will discuss the audit results of two domains that have been selected are DS5, DS9 and DS10. And from those results will be given a recommendation based on the existing gap between the current level and expected level.

4.1 DS5 Ensure Systems Security

Process description of this domain DS5 Ensure Systems Security is needed to maintain the integrity of information and protect Information Technology (IT) assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents. Analysis about

DS5 in Hospital is information system security is still being developed by hospitals. There is already planning from the hospital for the implementation of management information system in the future. Dependency on hospital information system has been realized and required by each hospital department. The security of hospital information systems is still dependent on the company that is the provider of information systems run in the hospital. Information system security problem is rare in Hospital and has been prevented to keep hospital data safe. Sensitive data is transmitted using Virtual Private Network (VPN). There has been regular monitoring activity by the hospital but there are no documentation and standard procedures for monitoring activities.

Gap Analysis is maturity level calculation result on the DS5 domain Ensure System Security gets an average of 2.54, level defined with the expected level 4, managed and measurable to produce a gap value of 1.46. To detail about DS5 Ensure Systems Security with sub-sub domains will be explained later.

4.1.1 DS5.1 Management of IT Security

Control Objectives for DS5.1 is manage IT security at the highest appropriate organizational level, so the management of security actions is in line with business requirements. Findings problem are IT security management is running well, and there are still some systems and processes controlled by vendors. Based on interviews, founded that the testing process on the level of security and monitoring of the system is not routinely performed. The testing process and its reports are not documented because there are no policies and procedures that require security checks. Maturity level of the DS5.1 processes was in level 3, defined.

Recommendations for sub-domain DS5.1 are management of hospital especially in the IT department has a division of tasks on each staff of the IT management so that the structure to organize and manage the system is running well. Provide written procedures to monitor and maintain the IT system well. Evaluate the planning that has been done every week once, this is done to avoid the occurrence of problems. Back up data on each division if you want to transfer data to the server, so that if the reception of data to the server has errors then the data is safe in the backup by the related division.

4.1.2 DS5.2 IT Security Plan

Control Objectives for DS5.2 is ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Findings problem are planning for IT security is quite good, the auditor does not find, documents related to

the IT Security Plan. Protection technology is done well enough, by installing a security gate firewall, capable of organizing and filtering data from the outside into, it's just that the policy setting process in the tool is not set or standardized in a standard policy. Maturity level of the DS5.2 processes were in level 2, Repeatable but Intuitive.

Recommendations for sub-domain DS5.2 are upgrade software by performing scheduling on a scale to update the system. Recording evaluation or documentation based on established procedures. Hospital should pay attention to server layout that is not very supportive because it is vulnerable to water or shocks. Provide additional closed circuit television (CCTV) or provide a level of security access rights to data processing, by changing the password once for every month.

4.1.3 DS5.3 Identity Management

Control Objectives for DS5.3 is ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Finding problem are information system used by the hospital when accessing it using only IP address. In this feature the company has not developed for the stage of ID and Password login because it is still in evaluation with the IT. There is no physical documentation of data regarding the user identity of the system. Maturity level of the DS5.3 processes was in level 3, defined.

Recommendations for sub-domain DS5.3 are IT Department already gives the user log in, but this user identity is only part of it attached to the company's division area. IT must have created a system of identity both internal and external so that things that are not desirable can be prevented. Update user identity data every single month to avoid data leakage. To additional of tools such as face detection on each computer so that IT staff can double the level of security in the company.

4.1.4 DS5.4 User Account Management

Control Objectives for DS5.4 is address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Finding problem are hospital IT staff does not delete employee accounts that are not working in the company anymore. IT staff are responsible for the creation, assignment, publishing or modification of each account in the company's proprietary information system with the manager's permission and request. Manager provides data on account details created, modified or deleted to IT staff, then IT staff executes the requests. There is no documentation and written procedure for this activity. In the event of non-conformity with access rights, Manager usually finds out when conducting operational audit. Maturity level of the DS5.4 processes was in level 3, defined.

Recommendations for sub-domain DS5.4 are IT in the company should make written procedures for the deletion and creation of user permissions or access rights for training in the company. IT must check user account to know that this user account is active or inactive. It is best to create user permissions gradually by asking users questions to complete the security process on the account. The issuance of permissions should be done on the same day, so there is no waiting time for each other.

4.1.5DS5.5 Security Testing, Surveillance, and Monitoring

Control Objectives for DS5.5 is IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. Finding problem are an update on IT security is only done when there is a really big problem. For checking IT staff is also not routinely responsible for this activity. There is no standard procedure or documentation done. TI does not provide standard procedure guides. Maturity level of the DS5.5 processes was in level 2, repeatable but intuitive.

Recommendations for sub-domain DS5.5 is IT should test and monitor in the implementation of IT security in a proactive manner, so that IT security can be well organized and appropriate supervision from IT staff and the manager. Companies must add security to the installation of CCTV to each department that can monitor the user's computer in the company, and logging functions that are always supervised by IT staff and managers in each department.

4.1.6 DS5.6 Security Incident Definition

Control Objectives for DS5.6 is clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process. Finding problem are the definition of a problem is not done formally and is done only by verbal communication between the IT staff and the users of the system. The one used to tackle the problem is only verbally defined and there is no documentation of the problem. Maturity level of the DS5.6 processes was in level 4, managed and measureable.

Recommendations for sub-domain DS5.6 are IT room in the company that the room is in terms of air circulation in the room is very crowd because of the frequent drops of water caused by the leakage of air conditioning hose, should the company fix and make a pipe path for air conditioning hose. For server lying should not be too low on the floor surface at least 10cm above the floor surface. Create security procedures in case of natural disasters such as earthquakes. In the event of electric shock or spark, preferably in the IT room provided fire extinguishers or immediately made a fire detector device in the ceiling.

4.1.7 DS5.7 Protection of Security Technology

Control Objectives for DS5.7 is make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily. Finding problem are for security technologies are usually updated and maintained regularly and usually once a year to improve the security. There is neither good procedure nor formal documentation for this activity. Maturity level of the DS5.7 processes was in level 2, repeatable but intuitive.

Recommendations for sub-domain DS5.7 are IT staff should always upgrade technology security in the company, such as the addition of face detection system, installation of print fingers, and the manufacture of Electric cards to enter the room every division. Documentation of the evaluation contained in the company.

4.1.8 DS5.8 Cryptographic Key management

Control Objectives for DS5.8 is determine that policies

and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure. Finding problem is cryptography for the disposal of unused data. No cryptographic keys are available for storing, modifying, using, distributing or deleting data, but IT is planning to create a cryptographic key. Maturity level of the DS5.8 processes was in level 3, defined.

Recommendations for sub-domain DS5.8 are create a written procedure on the provision of using cryptographic keys to organize and modify a data. Managers and IT staff must work together to avoid the practice of cheating or breaking of cryptographic keys using banned software. By limiting Internet access rights to every division except IT Staff. Perform documentation gradually and consistently.

4.1.9 DS5.9 Malicious Software Prevention, Detection, and Correction

Control Objectives for DS5.9 is put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam). Finding problem are there are activities to prevent malware activity is scanning with antivirus, then prohibit the activities of downloading data on computer other than for operational requirement. Until now there is no problem caused by malware. There is no standard procedure for the use of this software, and no formal documentation of the activities record. Maturity level of the DS5.9 processes was in level 2, repeatable but intuitive.

Recommendations for sub-domain DS5.9 are perform regular scans in accordance with established procedures and upgraded anti-virus software. Limit Internet permissions on every department, in order to avoid the occurrence of malware coming from the internet. Disable USB port or cable of data; avoid data transfer via external media on every computer in the company.

4.1.10 DS5.10 Network Security

Control Objectives for DS5.10 is Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks. Finding problem are there is a network conducted by the hospital, which uses a firewall and limit the use of Internet network on the computer used. There is no documentation or standard procedure for this activity. Maturity level of the DS5.10 processes was in level 2, repeatable but intuitive.

Recommendations for sub-domain DS5.10 are use security techniques and firewall related management procedures, network segmentation security equipment to authorize access and control information flow from user to network. Use the server computer specifications and also the user's computer as needed. Ensure the design of the computer network topology, by physically running the location of the network.

4.1.11 DS5.11 Exchange of Sensitive Data

Control Objectives for DS5.11 is Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin. Finding problem are sensitive data storage is less secure, because everyone can access it because of the lack of password. To exchange data between departments, the hospital uses a local network connected to a central computer. At the hospital, no standard procedure is established to regulate the exchange of data between departments, while for exchanging data with outside parties the staff follows the procedures and requirements provided by the parties outside of it. For documentation, staff reports on daily transactions. Maturity level of the DS5.11 processes was in level 2, repeatable but intuitive.

Recommendations for sub-domain DS5.11 are data security administratively needs to be done to maintain data security from insider or outsider intrusion. Training for staff to know the data security policies and procedures that must be carried out, by adding authentication tools, one form of identification to assure that the person who is communicating with us is a trusted and true person.

4.2 DS9 Manage the Configuration

Process description this domain is ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly. Analyses about DS9 in Hospital are has a repository for storing information about configuration items. IT staff is responsible for monitoring and configuration maintenance. All activities pertaining to configuration changes are logged. Logs can be opened by IT staff when there is a problem. The awareness of IT staff is important in managing these configurations, but there is still no routine documentation and standardized procedures for managing IT assets contained in the configuration repository. Configurations are not configured with change management, change Management, incidents and problems formally.

Gap Analysis is maturity level calculation result on the DS9 domain Manage the Configuration gets an average of 3.30, level defined with the expected level 4, managed and measurable to produce a gap value of 0.70. To detail about DS9 Manage the Configuration with sub-sub domains will be explained later.

4.2.1 DS9.1 Configuration Repository and Baseline

Control Objectives for DS9.1 is establish a supporting tool and a central repository to contain all relevant information on configuration items. Finding problem are if there is a change in the information system used, then there is a log that records the changes. This log is stored by the IT department used in the event of a problem after the change is made. No formal procedure is created when configuration changes are made. Maturity level of the DS9.1 processes were in level 4, managed and measurable.

Recommendations for sub-domain DS9.1 are building support tools and centralized repositories to store all

relevant information from the configuration object. Make the checkpoint a place of return when it occurs when a problem occurs. IT should have documentation for the monitoring process undertaken.

4.2.2 DS9.2 Identification and Maintenance of Configuration Items

Control Objectives for DS9.2 is integrate these procedures with change management, incident management and problem management procedures. Finding problem are there is no standard procedure or documentation to support configuration. Usually IT staff does it manually and not necessarily when in carry out. Maturity level of the DS9.2 processes was in level 3, defined.

Recommendations for sub-domain DS9.2 are establish formal procedures aimed at configuring the records performed by management on changes to the configuration repository. Build and manage complete repositories and subscriptions of baselines and asset configuration attributes and compare with actual asset configurations.

4.2.3 DS9.3 Identification Integrity Review

Control Objectives for DS9.3 is periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Finding problem are there is no regular review of the software installed on the computer. IT staff ensure that all licensed software is active and can be used properly. No normal logging is performed for configuration so there is no comparison of initial and final configuration. Maturity level of the DS9.3 processes was in level 3, defined.

Recommendations for sub-domain DS9.3 are often review the software that is installed against the rules of the use of the software in order to be able to identify that genuine or pirated software under the applicable license. Report and perform follow-up actions on issues that occur and justify the errors that occur. Documentation of configuration review on a system.

4.3 DS10 Manage Problem

Process description this domain are effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximizes system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction. Analysis about DS10 in Hospital is when a problem occurs on the system, the IT staff responsible for improving the system. If there are multiple system problems occurring at the same time, IT staff prioritizes the most pressing issues, usually the department is the most prioritized by IT staff. In the event of an operational problem, the IT Officer opens the log book to find out who should be responsible for the problem. Already there are multiple ways of solving the problem. The absence of written standard procedures and documentation on the problems that occur and the alternatives used. Problem solving is done by IT staff that is on duty according to their ability.

Gap Analysis is maturity level calculation result on the DS10 domain Manage Problem gets an average of 3.50, level managed and measurable with the expected level 4, managed and measurable, this domain equal between as is and expected . To detail about DS9 Manage Problem with sub-sub domains will be explained later.

4.3.1 DS10.1 Identification and Clarification of Problems

Control Objectives for DS10.1 is the steps involved in problem classification are similar to the steps in classifying incidents; they are to determine category, impact, urgency and priority. Finding problem are there is categorization of the problem, such as categorization of software, hardware, or network problems. IT at the company always responds to problems that occur. IT is also reviewing directly problems are going on. If the problem is a small problem then IT does not have a meeting between managers to make changes. Maturity level of the DS10.1 processes was in level 4, managed and measureable.

Recommendations for sub-domain DS10.1 are recording, tracking, resolving operational issues, checking root causes of all significant issues and defining solutions to operational problems on a scale and regular basis. Make the documentation and evaluation flow in the event of an accurate problem and create a sharing schedule for problem solving based on the group already collected.

4.3.2 DS10.2 Problem Tracking and Resolution

Control Objectives for DS10.2 is Ensure that the problem management system provides for adequate audit trail facilities that allow tracking, analyzing and determining the root cause of all reported problems. Finding problem are there is no special feature created by the company to identify problems that occur in the information system, but there are logs that can be used to locate the root of the problem, for example if there is a problem with the system update, then the IT staff opens the log to see what changes are causing the problem and do restore when needed. Maturity level of the DS10.2 processes was in level 3, defined.

Recommendations for sub-domain DS10.2 are establish a management system that has adequate audit trail facilities to assist with tracking and problem analysis. Periodically reports of change management from the progress of the problem analysis process error. Often monitor and classify identification according to the procedures in place so that problems can be well managed.

4.3.3 DS10.3 Problem Closure

Control Objectives for DS10.3 is Put in place a procedure to close problem records either after confirmation of successful elimination of the known error or after agreement with the business on how to alternatively handle the problem. Finding problem are once the problem is solved, the IT staff usually evaluates the IT team to find ways to prevent the problem from recurring, but IT staff does this not according to the standard rules, TI does it according to their initiative. Maturity level of the DS10.3 processes was in level 3, defined.

Recommendations for sub-domain DS10.3 are auditor recommends the company to establish a formal procedure for the company to settle the issue report in a timely manner and in accordance with the confirmation and approval of the business in the company.

4.3.4 DS10.4 Integration of Configuration, Incident and Problem Management

Control Objectives for DS10.4 is integrate the related processes of configuration, incident and problem management to ensure effective management of problems and enable improvements. Finding problem are there is no standard procedure or documentation that contains integration between configuration, incidents, and issues, but IT staff has recorded per point only into complaints issued by the company. Maturity level of the DS10.4 processes were in level 4, managed and measurable.

Recommendations for sub-domain DS10.4 are management must integrate configuration, incidents or problems that occur so that management can assess the effectiveness of the problem and facilitate the development of problem-solving solutions. Table 2 to show Summary about domain DS5, DS9, DS10 and sub-sub process.

Table 2. Summary Domain and Sub-Sub process.

Sub-Domain	**Level**	**Sub-Domain**	**Level**
DS5.1	3	Average DS5	2.54
DS5.2	2	DS9.1	4
DS5.3	3	DS9.2	3
DS5.4	3	DS9.3	3
DS5.5	2	Average DS9	3.3
DS5.6	4	DS.10.1	4
DS5.7	2	DS.10.2	3
DS5.8	3	DS.10.3	3
DS5.9	2	DS10.4	4
DS5.10	2	Average DS10	3.5
DS5.11	2		

V. Conclusion

This paper aimed to investigate and audit of information systems at RSAL Mintohardjo using assessment of best practices from COBIT Framework. This research provides an overview evaluation of IT/IS in Hospital. Organizations should take into considerations the importance of IT/IS and its aspects such as: effectiveness, efficiency, functional unit of information technology, the data integrity, safeguarding assets, reliability, confidentiality, availability, and security in enhancing their performance and service.

The results of this research proved that the maturity level for the Hospital based on Delivery and Support domain average was at 2.54 (Defined) until 3.5 (Managed & Measurable). This means that Hospital already has the standard procedure formal and written communications to all stakeholders to be obeyed and done in daily activities and already has a number of indicators which serve as each target Application of information technology applications.

Acknowledgment

Paper IT Governance was done thanks to Mintohardjo RSAL which has given permission for writer to do research, special thanks to Dr. Henny Sumihar Siregar, M.H, as head of the clinical coverage department who has assisted in the process of granting permission for the implementation of research and Mr. Erwan Triwahjono as KASUBBAG LITBANG as a mentor and research resource.

References

[1] A. Preittigun, W. Chantatub, and S. Vatanasakdakul, “A Comparison between IT Governance Research and Concepts in COBIT 5,” International Journal of Research in Management & Technology, 2012, 2(6), pp.581-590.

[2] Harwikarya, M. Sadikin, D. Fitrianah, M. M. Sarinanto, I. Nurhaida, and A. R. Dwiyanto. “IS Strategic Plan for Higher Education Based on COBIT Assessment: A Case Study,” International Journal of Information and Education Technology, 2015, 5(8), pp. 629-633.

[3] J. F. Andry, and H. Hartono, “Performance Measurement of IT Based on COBIT Assessment: A Case Study,” Jurnal Sistem Informasi Indonesia (JSII), Association for Information Systems – Indonesia chapter (AISINDO), 2017, 2(1), pp. 1-13.

[4] IT Governance Institute. COBIT 4.1 Framework, Control Objective, Management Guidelines, Maturity Models, Rolling Meadows, IL 60008 USA: ITGI, 2007, Available: http://www.isaca.org.

[5] S. Zhang, and H. Fever, “An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model,” Journal of Economics, Business and Management, 2013, 1(4), pp. 391-395.

[6] J. F. Andry, “Process Capability Model Based on COBIT 5 Assessments (Case Study),” Jatisi, 2016, 3(1), pp. 23-33.

[7] R. A. Khther, and M. Othman, “COBIT Framework as a Guideline of Effective It Governance In Higher Education: A Review,” International Journal of Information Technology Convergence and Services (IJITCS), 2013, 3(1), pp. 21-29.

[8] I. D. Lacković, “Model for IT Governance Assessment in Banks Based on Integration of Control Functions,” International Conference Active Citizenship by Management, Knowledge Management & Innovation, 2013, pp. 439-444.

[9] J. F. Andry, “Audit of IT Governance Based on COBIT 5 Assessments: A Case Study,” Teknosi, 2016, 2(2), pp. 27-34.

[10] S. C. B. Barbosa, I. A. Rodello, and S. I. D. Padua, “Performance Measurement of Information Technology Governance in Brazilian Financial Institutions,” JISTEM - Journal of Information Systems and Technology Management Revista de Gestão da Tecnologia e Sistemas de Informação, 2014, 11(2), pp. 397-414.

[11] H. B. Abbas, and S. H. Bakry, “Assessment of IT governance in organizations: A simple integrated approach,” Computers in Human Behavior, 2014, (32), pp. 261-267.

[12] J. F. Andry, “Performance Measurement of Information Technology Governance: A Case Study,” Journal of Information Systems, 2016, 2(12), pp. 56-62.

[13] R. C. S. Hariyono, “Audit Sistem Informasi Menggunakan Framework COBIT 4.1 Pada Website Universitas Peradaban,” Jurnal SMART COMP, 2018, 7(1), pp. 234-239.

[14] M. Rubino, and F. Vitolla, “Corporate governance and the information system: How a Framework for IT Governance supports ERM,” Managerial Auditing Journal, 2014, 29(8), pp. 736-771.

[15] J. F. Andry, and K. Christianto, “Audit Mengunakan COBIT 4.1 dan COBIT 5 dengan Case study”, Teknosain, Edition-1, ISBN: 978-602-6324-95-5, 2018.

[16] S. B. Elshaddai, and J. F. Andry, “Audit Sistem Informasi Inventory Menggunakan Kerangka Kerja COBIT 5 Di PT. Everlight,” Ikraith-Informatika, 2018, 2(1), pp. 26-33.

[17] T. Pradini, and J. F. Andry, “Audit Sistem Informasi Front Office Pada World Hotel Menggunakan Kerangka Kerja COBIT 4.1,” Ikraith-Informatika, 2018, 2(1), pp. 18-25.

[18] H. Tanuwijaya, and R. Sarno, “Comparation of COBIT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals,” International Journal of Computer Science and Network Security, 2010, 10(6), pp. 80-92.

[19] S. T. Yousif, and H. Sulaiman, “Conceptual Framework for Successful IT-Governance for E-Government Services,” The 3rd National Graduate Conference, 2015, pp. 302-307.

[20] COBIT 4.1 Framework. Control Objective, Management Guidelines, Maturity Models, Rolling Meadows, IL 60008 USA: ITGI, 2007.

[21] J. F. Andry, J. S. Suroso, and D. Y. Bernanda, “Improving Quality of SMEs Information System Solution with ISO 9126”, Journal of

Theoretical and Applied Information Technology, Vol. 96, No. 14, pp. 4610-4620,2018.
[22] Wijaya, R., and Andry, J. F. Performance measurement of JP Soft Application Using COBIT 5 Framework. Jurnal Ilmiah Teknologi Sistem Informasi, 2017, 3(2), 83-93.

J. F. Andry is a Senior lecturer in Department of Information System, Faculty of Technology and Design, Bunda Mulia University, Jakarta, Indonesia. He received his Master of Computer Science from Budi Luhur University in 2006. His research interests are in the area of Audit, Information System and Software Testing.

He has publish article in 9th International Seminar on Industrial Engineering & Management, Science, and Computer Science Education 2016, 2nd International Conference on Innovative Research Across Disciplines (ICIRAD 2017), and Journal of Theoretical and Applied Information Technology indexed by Scopus with title Improving Quality of SMEs Information System Solution with ISO 9126 and International Journal of Innovative Science and Research Technology with title Conceptual Framework for Successful IT-Governance and BSC for Service Industry and more journal such as journal Teknologi dan Sistem Informasi (TEKNOSI), Jurnal Sistem Informasi Universitas Indonesia, etc