Information Technology Audit For Management Evaluation Using COBIT and IT Security

(Case Study On Dishubkominfo of North Maluku Provincial Government, Indonesia)

Assaf Arief
Department of Information Engineering
Universitas Khairun
Ternate, Indonesia
assafarief83@gmail.com

Iis Hamsir Ayub Wahab
Department of Electrical Engineering
Universitas Khairun
Ternate, Indonesia
hamsir@unkhair.ac.id

***Abstract*— in modern organizational, the use of information technology to support the achievement of organizational and business goals must be balanced with the effectiveness and efficiency of its management. Information technology infrastructure available in Dishubkominfo the Provincial Government of North Maluku Indonesia has not been optimized, the problem of lack of human resources to lead and management of information technology is not well managed and also the absence of control over the level of information technology security. This condition makes the direction of government policy in the field of Information Technology is not clear. Required a mechanisms information technology control so that measurable what has been done both advantages and disadvantages of the government's rules and policies are in accordance with international standards. This study uses the two frameworks: COBIT 5 and IT Security for Information Technology Audit. The Information Technology audit results of Dishubkominfo institution has the maturity level of information technology management at level 2 are Repeatable but Intuitive controls for mapping and principle of COBIT 5, while the average score of information security standard ISO/IEC 17799:2005 was 39%. The results of data processing to find value - average for the domain APO and MEA was 1.71 and the value - average for principle is 1.98 latter value - average for the maturity level of information security standard ISO/IEC 17799:2005 is 31 or 39%, which means that the security of information technology is still very less and should be highly improved.**

Keywords: COBIT 5, ISO/IEC: 17799:2005, IT Security, IT Management, Dishubkominfo of North Maluku.

I. INTRODUCTION

Dependence on information technology (IT) is a characteristic common to virtually all modern organizations including local government. The utilization of IT governance in government organizations at central and regional levels will ensure the improvement of efficiency, effectiveness, transparency, and accountability in good governance[1].

IT Governance success is determined by the alignment of the application of IT and organizational objectives. IT alignment becomes an important issue in strategy development and organizational performance improvement to define organizational strategy and operate the organization in a way intended to help realize its business goals and objectives[2]. The various models of IT governance best practices in the world has been widely introduced, such as : The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), IT Security, National Institute of Standards and Technology (NIST), the British Standards Institution (BSI) Baselines, ISO/IEC 27002, ISO/IEC 385000, and others. Each has its advantages and disadvantages [3].

The use of information technology must be balanced with proper regulation and management so that the disadvantages that may occur could be avoided. Disadvantages in question may in the form of inaccurate information caused by incorrect data processing so that it can influence the decision was wrong. IT asset security one of which is the data is not maintained, the integrity of the data that cannot be maintained, these are the things that can affect the effectiveness and efficiency in achieving the organization's goals and strategies. In connection with the reasons required the existence of a mechanism of control over the management of information technology[4].

In addition to the above-mentioned, there are some problems that appear in designing information technology governance in local government. How to control the information technology risk management at the operational level and designing information technology in mapping an integrated framework. So this led to the adoption of information technology in local government to be inefficient[5]. The Department of Transportation, Communications and Informatics (Dishubkominfo) of North Maluku provincial government in this regard management information systems and communication sector which are housed in Sofifi an institution that has a vision of service delivery of reliable, competitive and provide value-added[6]. However, available information technology infrastructure is not yet fully optimized, the lack of human resources to manage lead management of information technology is not managed properly. Lack of control over the level of information technology security. This condition makes the policy direction is not clear[1][4].

Audit of IT governance has not been done for the initial mapping of field conditions. That's necessary to map the beginning of an information technology audit control mechanisms so that later the measurement results obtained maturity level of the organization and recommendations are based on the COBIT 5 framework and IT Security. This is to provide evaluation and feedback that can be used for improvements in its management in the future and help secure information technology assets in a professional manner.

II. LITERATURE REVIEW

A. IT Governance

The term *governance* in business contexts refers generally to the set of policies, processes, and actions taken by management to define organizational strategy and operate the organization in a way intended to help realize its business goals and objectives. In contrast, *IT governance* refers to the structure and processes organizations use to try to ensure that their IT operations support the overall goals and Objectives of the organization. According to the IT Governance Institute, governance objectives applicable to virtually any organization include aligning IT strategy with enterprise strategy, allocating IT resources efficiently to support the achievement of organizational objectives and realize the value anticipated from IT investments, and effectively managing IT-related risk [2]. With the addition of performance measurement to allow organizations to assess to what extent they are achieving their objectives, IT governance comprises the management functions as depicted in Fig.1.

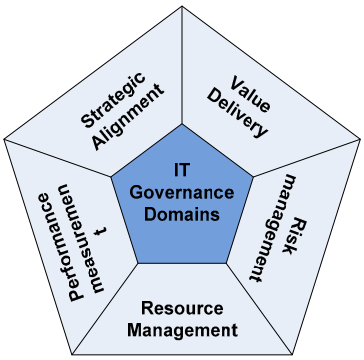

Fig.1. IT Governance Focus Area[7]

B. COBIT 5

The latest version of COBIT, COBIT 5 [8], is recently introduced. Thus, an analysis and comparison of COBIT 5 concepts and existing literature may help researchers understand the gap between the practical world and academic world. COBIT 5 is new and has a limited number of academic literature that discussed it[9]. COBIT 5 is introduced as a framework for "Enterprise governance of IT" rather than "IT Governance". Enterprise governance of IT shares similar concept to IT governance but it emphasizes the involvement and responsibility of business side rather than technical side[9]. COBIT 5 is designed to be a single integrated framework that can be used for both governance and management[8]. COBIT 5 defines governance as: "Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making, and monitoring performance and compliance against agreed-on direction and objectives" [8]. COBIT 5 Principles shown in Fig.2.

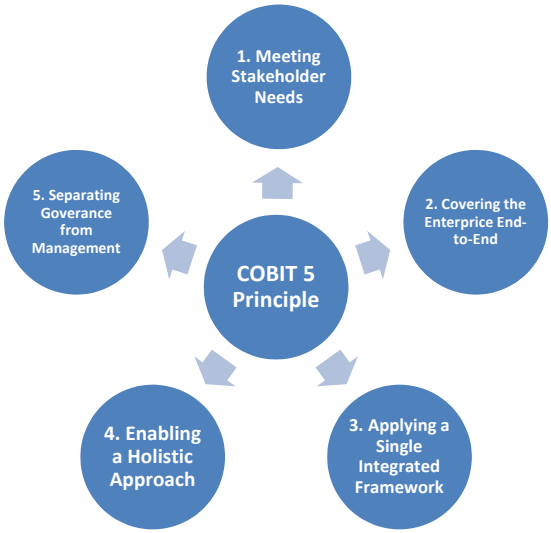

Fig. 2. COBIT 5 Principles [8]

C. Maturity Model

COBIT view that implementing effective governance mechanism is not easy, but must go through various stages of maturity specific. Maturity model to control IT processes, so that management can determine where to position the organization now, and positioned where the organization wants to be. At least the position of the maturity of an organization associated with the availability and performance of IT governance processes can be categorized into six levels that shown in Table.1. The purpose maturity level are [10]:

1. Organizations can determine the position of Information Technology maturity at this time.
2. The organization is continuous and sustainable should endeavor to increase the level to the highest level so that the governance aspects of Information Technology can run effectively.

TABLE.1. MATURITY MODEL SCORING

Incomplete	Performed	Managed	Established	Predictable	Optimizing
0	*1*	*2*	*3*	*4*	*5*
To solve ASP	*To solve*	*To Improve*	*Acceptable*	*Good*	*Excellent*

D. IT Security

According to ISO/IEC 17799:2005 on an information security management system that information security is the protection of a wide range of threats to ensure business continuity, minimize business risk and improve the investment and business opportunities[11].

Security Information Technology or IT Security refers to an effort to secure the information technology infrastructure of the disturbances in the form of illegal access and network utilization which is not allowed.

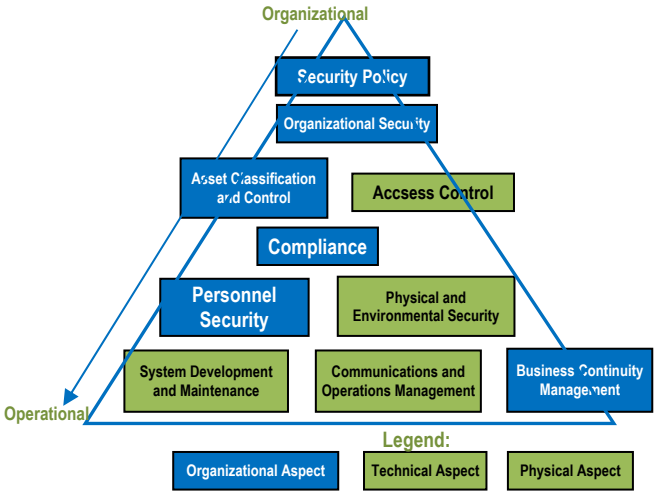

Fig. 4. The Ten Domain of ISO/IEC 17799:2005[11]

III. Research Methods

The method used in this study is a qualitative methodology research procedures that produce descriptive data in the form of words written or spoken of people and behaviors that can be observed. Collecting data of the population that can be measured, in an economical way with involving the use of questionnaires and interviews[12]. In this study, the objects and materials research are employees of Department Transportation, Communication and Information (Dishubkominfo) of North Maluku Provincial Government, Indonesia.

A. Data Collecting Methods

Prepare a list of questions in the form of a questionnaire document. Questionnaire in this study was designed to determine the maturity level of information technology management and security levels of information technology that has been used by a government agency to look at user feedback, rules and decision-making in implementing the technology in Dishubkominfo.

Data collecting methods used in the questionnaire are closed ended question based on the principle of COBIT and ISO/IEC 17799:2005. The sampling technique of COBIT used in this research is measured using a random sampling of five maturity level point score ranging from 0 (incomplete) to 5 (Optimizing) and the sampling technique of IT Security based on ISO/IEC 17799:2005 using a random sampling of ten security index point with Yes or NO answer.

B. Data Analysis Methods

Data processing in the study through the following stages are 1) Inspection data and making symbols, 2) Mapping to COBIT 5 and 3) Mapping to IT Security based on ISO / IES 17799:2005.

1) Inspection data and making symbols

The analysis was conducted by reviewing the results of the election control objective has been done through a questionnaire, so it can be deduced, shown in Table 4.

TABEL 4. IT PROCESS DESCRIPTION

IT Domain	*IT Process*
Align, Plan, and Organise	***APO1,APO2,APO3,APO7,APO11***
Monitor, Evaluate, and Assess	***MEA1***

2) Mapping to COBIT 5

COBIT 5 Principles focus are: 1) Meeting Stakeholder Needs, 2) Covering the Enterprise End-to-End, 3) Applying a Single Integrated Framework, 4) Enabling a Holistic Approach, 5) Separating Governance From Management. COBIT 5 Process capability assessment model to assessment model shown in Table 5.

TABEL 5. COBIT 5 PROCESS CAPABILITY ASSESSMENT MODEL[13]

COBIT 5 Process Capability Assessment Model (PAM)			
0	Incomplete	*Performance Attribute (PA)*	
1	Performed	PA1.1	Process Performance
2	Managed	PA2.1	Performance Management
		PA2.2	Work Product Management
3	Established	PA3.1	Process Definition
		PA3.2	Process Deployment
4	Predictable	PA4.1	Process Measurement
		PA4.2	Process Control
5	Optimizing	PA5.1	Process Innovation
		PA5.2	Process Optimization

3) Mapping to ISO/IEC 1799:2005

The ten aspects (**A1 - A10**) to be assessed on the security of information technology base on ISO/IEC 1799:2005 are:

a. Security Policy (**A1**)
b. Organization Security (**A2**)
c. Asset Classification and Control (**A3**)
d. Access Control (**A4**)
e. Compliance (**A5**)
f. Personnel Security (**A6**)
g. Physical and Environmental Security (**A7**)

h. System Development and Maintenance (**A8**)
i. Communications and Operations Management (**A9**)
j. Business Continuity Management (**A10**)

IV. Results and Discussion

The Preliminary results of an audit research data processing using the entire capability assessment process model of COBIT 5 of this paper are new only two control domains APO and MEA1 because other aspects of the assessment based on COBIT 5 are almost nonexistent. Two domains that are used for IT Audit in Department (Dishubkominfo) as shown in Table 6.

TABLE. 6. TWO DOMAIN CONTROL OF EVALUATING

Domain	***Practice (Align, Plan, and Organise)***
APO1	*Manage the IT Management Framework*
APO2	*Manage Strategy*
APO3	*Manage Enterprise Architecture*
APO7	*Manage Human Resource*
APO11	*Manage Quality*
Domain	***Practice (Monitor, Evaluate. And Assess)***
MEA1	*Monitor, Evaluate and Assess Performance and Corformance*

The present condition of information technology audit management in Dishubkominfo now can be identified through the analysis of the maturity level that refers to a particular two domain of COBIT is APO1, APO2, APO3, APO7, APO11 and MEA1 delivery and support as well as monitoring and evaluation domain. The maturity level result scores calculation results as shown by the chart Fig. 5.

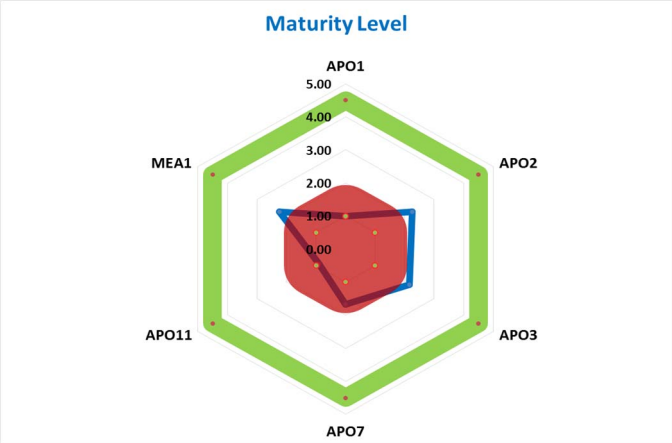

Fig. 5. The Maturity Level Result

From Fig. 5 with the maturity level chart based on two control COBIT (APO1, APO2, APO3, APO7, APO11 and MEA1) mapping above shows that; value - average for the domain APO and MEA was 1.71 and the value - average for principle is 1.98 if the result is rounded to level 2 means repeatable but Intuitive (managed). A score of 4.00 is the maturity level expected. The results of the assessment are expected maturity level aims to provide a reference for the development of information technology management in Dishubkominfo Government of North Maluku. The blue line on the chart shows the value score maturity level of the organization at this time, while the red circle indicates a low value / bad zone and should be evaluated. For the green line shows the target organization wants to achieve in the future.

The value score maturity level is an evaluation tool for analyzing the degree of readiness of information technology management in government agencies. This evaluation tool is not intended to analyze the appropriateness or effectiveness of existing security form, but rather as a tool to provide an overview of readiness condition (completeness and maturity index) governance framework of information to the leadership of institutions. The department (Dishubkominfo of North Maluku) focus in 2016 was on the implementation and improvement of transportation so that the funds in the improvement and development of information technology is limited. So that an assessment should be done gradually to achieve a score of 5 (optimizing).

Whereas, for the results of the calculation of the percentage rate of the ISO 17799 Information Security standard is described in Table 7 below.

TABLE 7. THE TEN ASPECT DOMAIN OF ISO/IEC 17799:2005

Aspects	**Description**	KTI Level	
		Yes Answer Freq.	(%)
A1	Establish an information security policy to secure and maintain the integrity of crucial information.	**2**	**25%**
A2	Organizing security to manage information security within an organization.	**4**	**50%**
A3	The classification and control of assets to maintain the proper protection for the organization.	**4**	**50%**
A4	Do security personnel to reduce the risk of human error, theft, fraud or misuse of facilities.	**3**	**38%**
A5	Control the physical and environmental security to prevent unauthorized access, damage and interference to business premises and information	**2**	**25%**
A6	Communication and operations management to ensure that the information processing facility running correctly and safely	**5**	**63%**
A7	Controlling access to prevent unauthorized access to information systems	**3**	**38%**
A8	Conducting development and maintenance of the system to ensure that security is built into information systems	**3**	**38%**
A9	Set the business continuity management to face the possibility of termination of business activities and to protect critical business processes from failure and major disasters.	**1**	**13%**
A10	Doing suitability in order to avoid a violation of criminal and civil law, statutory, regulatory or contractual obligations as well as other security provisions.	**4**	**50%**
	Average	**31**	**39%**

The results of the security evaluation index illustrate the level of maturity, the level of completeness of the application of ISO/IEC 17799: 2005, and a map of the area of information systems security governance in an organization by using the ten aspects of the domain. As an illustration, the results of a security index evaluation index shown in Fig 6.

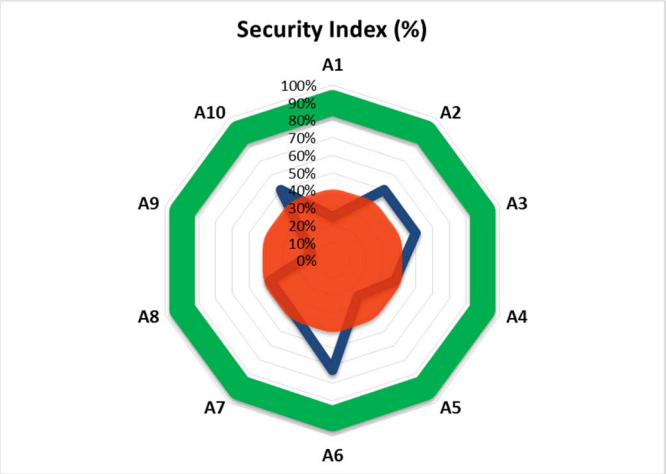

Fig. 6. The Security Index Result

From Fig. 6 with the security index chart of ten aspects of ISO/IEC 17799:2005 (A1 to A10) mapping above shows that; the value - average for the maturity level of information security standard ISO/IEC 17799:2005 is 31 or 39%, which means that the security of information technology is still very less and should be much improved. A high score of 63% in communication and operations management aspects and 13% in business continuity management aspects. That shown in the blue line on the chart shows the value score security index of the organization at this time, while the red circle indicates a low value / bad zone and should be evaluated. For the green line shows the target organization wants to achieve in the future.

V. Conclusion and Future Work

After analysis and calculation of maturity level in the present study may be that the level of maturity of IT governance on two domain based framework COBIT in Dishubkominfo North Maluku Provincial Government received an average score of i.e. 1.71 = 2 (rounded up) means in maturity level are managed and to improve. These values are means still much to be improved and enhanced in order to meet the standards of good IT governance for public service. While the aspect of IT security is based on the standard ISO/IEC 1799:2005, scored an average percentage of 39% security index, meaning that they must continue to be improved and prepared on the security aspects of IT governance.

For the future work in this study to be more comprehensive to use all aspects of the assessment of controls on COBIT 5 and using the latest ISO standards of security for IT governance on Dishubkominfo of North Maluku Provincial Government, Indonesia. The results of the evaluation and analysis are not intended to analyze the appropriateness or effectiveness of the existing form of governance, but rather as a tool to provide an overview of readiness condition (completeness and maturity) framework for IT governance to the head of the institution for the better in the implementation of IT governance.

Acknowledgment

The authors would like to thank Governor of North Maluku Government, Indonesia. This work was supported by Directorate General of Higher Education (DIKTI) of Indonesia, Department of Informatics Engineering and Department of Electrical Engineering of Universitas Khairun. Also, special thanks to Laboratory of Software Engineering, Faculty Engineering, Universitas Khairun, Indonesia.

References

[1] Departemen Komunikasi dan Informatika, "*Panduan Umum Tata Kelola TIK Nasional*," vol. 1, 2007, pp. 1–49.
[2] S. D. Gantz and S. Maske, *The Basics of IT Audit Practical Information*. Elsevier Inc., 2014.
[3] S. De Haes, W. Van Grembergen, and R. S. Debreceny, "*COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities*.," *J. Inf. Syst.*, vol. 27, no. 1, pp. 307–324, 2013.
[4] Tim Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika RI, *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*, 2.0, Sept. Jakarta, 2011.
[5] I. H. A. Wahab and A. Arief, "*An integrative framework of COBIT and TOGAF for designing IT governance in local government*," in *2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2015, pp. 36–40.
[6] Biro Humas dan Protokoler Setda Provinsi Maluku Utara, *Rencana Strategis (RENSTRA) Biro Humas dan Protokoler*, vol. 1. 2015.
[7] K. Brand and H. Boonen, *IT Governance based on COBIT 4.1-A Management Guide*, Third edit. ITSMF Library, 2007.
[8] Isaca, *A Business Framework for the Governance and Management of Enterprise IT*. 2012.
[9] A. Preittigun and W. Chantatub, "*A Comparison between IT Governance Research and Concepts in COBIT 5*," *Int. J. Res. Manag. Technol.*, vol. 2, no. 6, pp. 581–590, 2012.
[10] S. Wardani and M. Puspitasari, "Audit Tata Kelola Teknologi Informasi Mengunakan Framework COBIT Dengan Model Maturity Level (Studi Kasus Fakultas ABC)," *J. Teknol.*, vol. 7, no. 1, pp. 38–46, 2014.
[11] M. Syafrizal, "*ISO 17799 : Standard Sistem Manajemen Keamanan Informasi*," in *Seminar Nasional Teknologi 2007 (SNT 2007)*, 2007, vol. 2007, no. November, pp. 1–12.
[12] C. W. Dawson, *Projects in Computing and Information Systems*, vol. 2. 2009.
[13] P. Copy and M. Starr, *Self-assessment Guide: Using COBIT ® 5*. 2013.