

Application of COBIT 5 for Hospital Services Management Information System Audit

Ida Bagus Leo Mahadya Suta^{1*}, I Gusti Ngurah Agung Surya Mahendra², and Made Sudarma³

^{1,2}Department of Electrical and Computer Engineering, Post Graduate Program, Udayana University

³Department of Electrical and Computer Engineering, Udayana University

*gusleo.bali@gmail.com

Abstract We conduct research on hospital management information system management audits where management includes services to patient queuing times and medical personnel who implement COBIT 5 with the Deliver, Service, Support (DSS) domain from the results of the application of DSS domains on COBIT 5 then maturity levels are obtained an average of 2.2 to 2.8 who have an IT governance process in hospital services has a pattern that is repeatedly performed.

Keywords — COBIT 5, Hospital Service Information Management System, Deliver, Service, Support, DSS.

I. INTRODUCTION

The application of information and communication technology has now become a necessity and demand for every public service provider agency. A hospital that is one of the public service providers and to realize good service to the community, it is necessary to manage a good information system. In the use of information systems in an agency, namely a hospital, of course, requires an internal control mechanism. Based on the regulation of the Minister of Communication and Information Number: 41 / PER / MEN / KOMINFO / 11/2007 concerning general guidelines for information technology and national communication governance states that "in order to support the objectives of government administration of public services, good information and communication technology plan is needed (good governance)" [1].

Hospital as one of the public facilities is expected to be able to provide Information System services optimally to the community. The use of hospital SIMRS (Hospital Management Information System) based on information technology will make it easier for people to carry out administrative and transaction processes [2]. But in reality in some hospital agencies, the use of SIMRS is not optimal, so long and repeated administration still occurs.

Comprehensive and continuous standards, procedures and work evaluations are needed with reference to one of the international standards in the form of COBIT 5 that will be able to create efficient and effective SIMRS. The

improvement framework of COBIT 4 to COBIT 5 helps companies gain the role in controlling IT related matters such as the development and management of IT governance [3].

The selection of COBIT 5 is appropriate for carrying out the information technology audit process because it covers all elements of information technology governance not centered solely on technical issues in technology but also sees other resources that drive information technology governance towards organizational goals. The domain used in this audit process is Deliver, Service, and Support (DSS) and performs the maturity test of each process from the domain using capability level [4].

II. LITERATURE REVIEW

A. Information System Audit

Information System Audit is the process of collecting and evaluating evidence to determine whether the computer system used has been able to protect the assets of the organization, is able to maintain data integrity, can help achieve organizational goals effectively, and use resources efficiently [5].

B. Information Technology Governance

IT governance is the responsibility of the board of directors and executive management. This is an integral part of corporate governance and consists of leadership and organizational structures and processes that ensure that IT organizations sustain and expand organizational strategies and objectives.

C. Hospital Management Information System

IT governance is the responsibility of the board of directors and executive management. This is an integral part of corporate governance and consists of leadership and organizational structures and processes that ensure that IT organizations sustain and expand organizational strategies and objectives.

D. COBIT 5

COBIT (Objective Control for Information and related Technology) is a corporate IT governance framework, in the form of a set of standard measurements for IT management. COBIT was developed by ISACA (Information System Audit and Control Association). (ISACA, 2002) COBIT 5 according to Fig. 1 is the latest version of COBIT, which combines COBIT 4.1, Val IT 2.0 and Risk IT. COBIT 5 is a strategic development that provides ISACA's next generation guidance on governance and management for enterprise information technology [6].

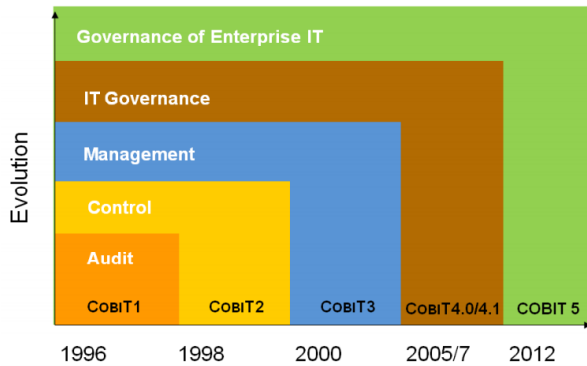


Fig. 1. Evolution of COBIT

COBIT 5 cascade goals is a mechanism to translate stakeholder needs into specific company objectives, can be followed up and adjusted, targets and targets related to IT. This translation allows the setting of specific objectives at each level and in each area of the company to support the overall goals and requirements of stakeholders, and thus effectively support alignment between company needs and IT solutions and services. (ISACA, 2002). Fig. 2 illustrates this.

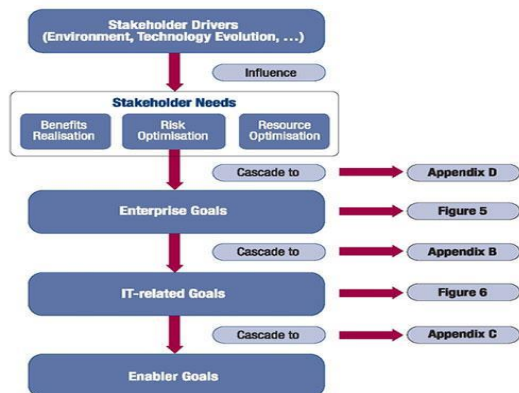


Fig. 2. Cascade Goals Scheme

COBIT 5 makes a clear distinction between governance and management and has 5 domains namely Evaluate, Direct, and Monitor (EDM), Align, Plan, and Organize (APO), Build, Acquire, and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate, and Assess (MEA). Total processes that exist in corporate governance and IT management with 37 process details. (ISACA, 2003). Fig. 3 illustrates this.

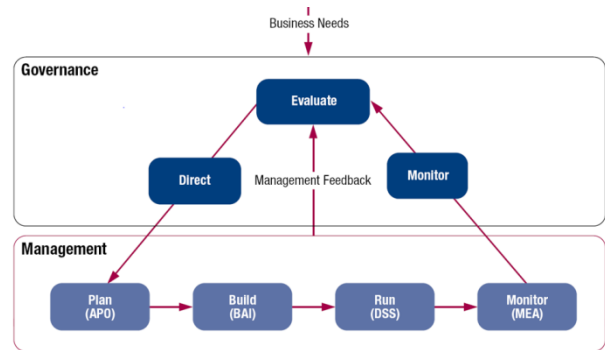


Fig. 3. Governance and management area

III. METHODOLOGY

A. Method of collecting data

To carry out the activities of the supervision process, evaluation and evaluation of the performance of IT data processing in the COBIT 5 framework there are guidelines. The method of data collection according to the COBIT indicator is the information technology performance evaluation process using questionnaires which are strengthened by the method of interviews, observations, and related literature studies.

1) Interview

Interviews were used to test the correctness and maturity of data and obtain more complete data from the questionnaire method. This interview method is in accordance with the guidelines for the model of the level of capability of COBIT control Objectives 5.

2) Observation

Observation is a method of data collection that is done by observing directly by looking at and retrieving data needed in the place where the research is conducted. Data collection was carried out at **the Hospital of Ganesha Celuk – Gianyar, Bali** directly, such as seeing how the information system is running. In addition, it is also used to see the description of which parties have an interest in carrying out the expected activities.

3) Questionnaire

The method of data collection uses a questionnaire in this study, namely a questionnaire regarding capability level. To measure the extent of the level of monitoring capability, evaluation and suitability of information technology performance applied to **the Hospital of Ganesha Celuk – Gianyar, Bali** within the framework of COBIT 5 performance.

4) Literature and written documents

The library method and written documentation in this study are studying books and other sources of information related to the topic of discussion to gain an understanding of the subject and object to be studied. In addition, written documents are also needed relating to the implementation of information system monitoring and evaluation in the Hospital of Ganesha Celuk - Gianyar, Bali.

B. Analysis Method

In this study, COBIT-based measurement design was initially created, which is to determine what processes will be assessed based on the analysis of the Strategic Plan and IT operational policies and processes that exist in COBIT and carry out Management Awareness analysis. After determining what control objectives will be measured, in the form of the capability model questionnaire as a tool to measure the maturity level of IT processes based on the COBIT 5 framework. The entire process can be seen in Figure 4 which illustrates the following:

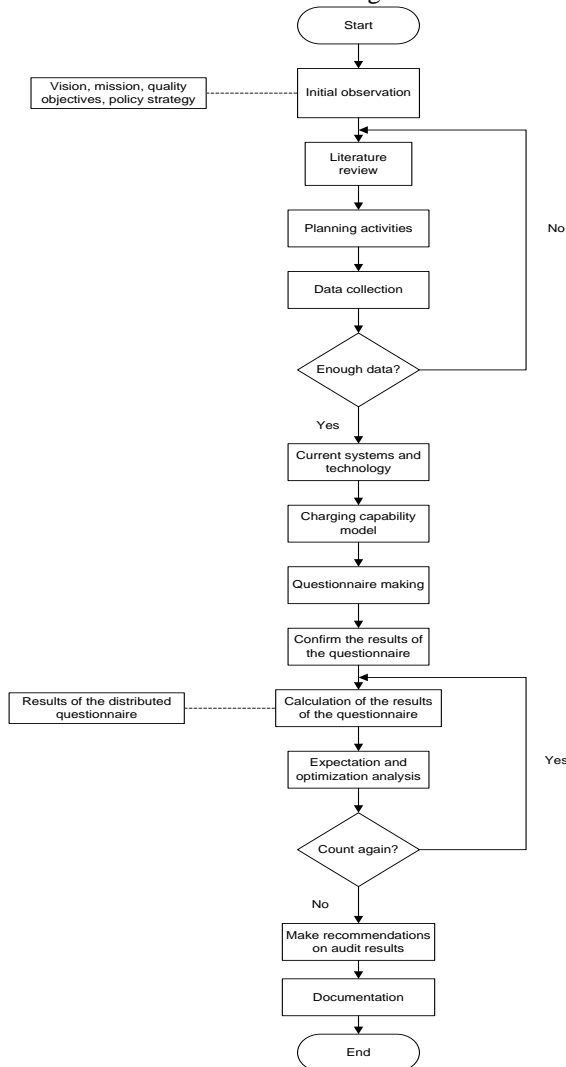


Fig 4. Research Methods

IV. RESULTS AND DISCUSSION

A. Recapitulation of Respondents

The target respondents to be used include several aspects of the section, including: Management, IT Users and IT Section itself. From these 3 parts, the following is the recapitulation of respondents based on the work part of them:

TABLE I
RECAPITULATION OF RESPONDENTS

#	Section Name	Total
1	Management	10 People
2	Operator	12 People
3	IT Support	2 People
3	Patient	20 People

B. COBIT Domain Mapping and Selection 5

COBIT 5 has provided guidelines for mapping and selecting Domains and processes so that the assessment is in accordance with the needs of the research conducted which of course refers to the strategic objectives of the research object in terms of optimizing the Queue Time Management and Service Design Information System and the Quality of Hospital Medical Power.

This domain selection process begins by looking at the objectivity of governance, namely resource optimization, this resource is related to the Management Information System and the Queue Time Service Design and Hospital Medical Quality in supporting the integration of health services. This can be seen in Table 1 below:

TABLE II
IDENTIFICATION OF STRATEGIC OBJECTIVES WITH BALANCE SCORE CARD

Balance Score Card Dimension	Strategic Goals
Finance	Adjustment of the use of facilities and infrastructure to the rapid development of information technology to improve health service activities
Customer	Produce innovations in the field of science and technology as a solution for sustainable development through research and other studies
Internal	Applying innovation in the field of science and technology as a solution in the form of community service to improve people's welfare
Learning and Growth	Improve the ability of health services Human Resources (HR) according to qualifications and development

The next process is choosing Corporate Goals (EG) by mapping the implementation of a balance score card (BSC) and selection of selected processes that have Primary signs in the object of governance, namely optimization of resources. selected, including 10 Primary categories (P) of company goals and 6 Secondary categories (S) of company goals.

TABLE III
SELECTED ENTERPRISE GOALS

Balance Score Card Dimension	Strategic Goals	Resource Optimisation
Finance	1. Stakeholder value of business investments	S
	2. Portfolio of competitive products and services	S
	3. Managed business risk (safeguarding of assets)	S
	4. Compliance with external laws and Regulations	S
	5. Financial Transparency	S
Customer	6. Customer-oriented service culture	p
	7. Business service continuity and availability	p
	8. Agile responses to a changing business Environment	p
	9. Information-based strategic decision making	p
	10. Optimisation of service delivery costs	p
Internal	11. Optimisation of business process Functionality	p
	12. Optimisation of business process costs	p
	13. Managed business change programmes	p
	14. Operational and staff productivity	p
	15. Compliance with internal policies	S
Learning and Growth	16. Skilled and motivated people	P
	17. Product and business innovation culture	P

The next process is the result of Mapping IT - Related Goals so that all of the mapping results will be mapped back to the process found in COBIT 5.

TABLE IV
MAPPING COBIT 5 IT - RELATED GOALS TO PROCESS

Cobit 5 Process	EG-01	EG-02	EG-03	EG-04	EG-05	EG-06	EG-07	EG-08	EG-09	EG-10	EG-11	EG-12	EG-13	EG-14	EG-15	EG-16	EG-17
	Finance					Customer					Internal					Learning & Growth	
DSS01				P			P				P						
DSS02				P			P										
DSS03				P			P				P				P		
DSS04				P			P								P		
DSS05		P		P													
DSS06				P			P										

The results of the above mapping make IT-Related Goals supported by processes in COBIT 5 so that the selection of processes can be tailored to strategic objectives which also support the process of hospital integration and tailored patients based on field needs. The following is the process of mapping the above process that is tailored to the needs of the hospital and the patient.

TABLE V

RESULTS OF MAPPING IT - RELATED GOAL WITH COBIT 5 PROCESS

IT Related Goals	COBIT 5 Process
02 - IT compliance and support for business compliance with external laws and regulations	DSS05
04 - Managed IT-released business risk	DSS01, DSS02, DSS03, DSS04, DSS05, DSS06
07 - Delivery of IT services in line with business requirements	DSS01, DSS02, DSS03, DSS04, DSS06
11 - Optimisation of IT assets, resources and capabilities	DSS01, DSS03
14 - Availability of reliable and useful information for decision making	DSS03, DSS04

C. Information System Maturity Level Measurement

Based on the results of the survey with the COBIT 5 questionnaire on the DSS domain, the results of the hospital service information system are drawn. The results of this description are obtained by calculating the level of capability to the application of information systems based on the results of the survey with the COBIT 5 questionnaire. The results are in the table as follows:

1) DSS01 Manage Operations

At this stage we will produce IT operational services according to plan, with a description of the process is to coordinate and carry out operational activities and procedures needed to provide internal IT services and outsourcing, including the implementation of predetermined standard operating procedures and monitoring activities required by the process capability model what is expected from DSS01 management operations, is level 4, a predictable process. In more detail are subdomains, see Table V. Ability to process DSS01 domains manage operations. It was concluded that the average DSS01 was at level 2.8, Managed Process.

TABLE VI
DSS01 PROCESS CAPABILITY DOMAIN MANAGE OPERATIONS

#	Sub Domain	Current	Expected
DSS01.01	Perform operational procedures	3	4
DSS01.02	Manage outsourced IT services	3	4
DSS01.03	Monitor IT infrastructure	2	4
DSS01.04	Manage the environment	3	4
DSS01.05	Manage facilities	3	4
Average		2.8	4

2) DSS02 Manage Service Requests and Incidents

In this step, we will analyze the achievement of productivity improvements and minimize disruptions through rapid resolution of user questions and incidents, with a description of the process providing a timely and effective response to user requests and resolution of all types of incidents. Improve normal service, record and fulfill user requests, and record, investigate, diagnose, improve and resolve incidents. The expected process capability model of DSS02 manages service requests and incidents is level 4, a predictable process. In more detail are subdomains, see Table VII. The ability of the DSS02 domain process manages

service requests and incidents. Concluding the average DSS02 is at level 2.3, Managed Process.

TABLE VII

DSS02 PROCESS CAPABILITY DOMAIN MANAGE SERVICE REQUESTS AND INCIDENTS

#	Sub Domain	Current	Expected
DSS02.01	Define incident service request	2	4
DSS02.02	Record, classify and prioritize requests and incidents	2	4
DSS02.03	Verify, approve and fulfill service requests	2	4
DSS02.04	Investigate, diagnose and allocate incidents	3	4
DSS02.05	Resolve and recover from incidents	2	4
DSS02.06	Close service requests and incidents	2	4
DSS02.07	Manage the environment	3	4
Average		2.3	4

3) DSS03 Manage Problem

At this stage, we will analyze increasing availability, improve service levels, reduce costs, and increase customer comfort and satisfaction by reducing the number of operational problems, with a description of the process of identifying and clarifying issues and root causes and providing timely resolutions to prevent repeated incidents. Give recommendations for improvement. The expected process capability model of DSS03 management problems is level 4, a predictable process. In more detail are subdomains, see Table VIII. The process of DSS03 domain capabilities manages problems. Concludes DSS03 on average at level 2.4, Managed Process.

TABLE VIII

DSS03 PROCESS CAPABILITY DOMAIN MANAGE PROBLEM

#	Sub Domain	Current	Expected
DSS03.01	Identity and classify problems	2	4
DSS03.02	Investigate and diagnose problems	2	4
DSS03.03	Raise known errors	3	4
DSS03.04	Resolve and close problems	3	4
DSS03.05	Perform proactive problem management	2	4
Average		2.4	4

4) DSS04 Manage Continuity

At this stage we will continue to analyze important business operations and maintain the availability of information at a level that can describe the company's processes in the event of a significant disruption, with a description of the process of establishing plans to improve business and IT responding to incidents and disruptions to continue important business process operations and need IT services and maintain the availability of information at a level acceptable to the company. The expected process capability model of DSS04 manages continuity is level 4, a predictable process. In more detail are the subdomains, see Table IX. The process capability of the DSS04 manage continuity domain. It was concluded that the average DSS04

was at level 2.5, Managed Process.

TABLE IX

DSS04 PROCESS CAPABILITY DOMAIN MANAGE CONTINUITY

#	Sub Domain	Current	Expected
DSS04.01	Define the business continuity policy, objectives and scope	3	4
DSS04.02	Maintain a continuity strategy	3	4
DSS04.03	Develop and implements a business continuity response	3	4
DSS04.04	Excercise, test and review the BCP	2	4
DSS04.05	Review, maintain and improve the continuity plan	2	4
DSS04.06	Conduct continuity plan training	2	4
DSS04.07	Manage backup arrangements	3	4
DSS04.08	Conduct post-resumption review	2	4
Average		2.5	4

5) DSS05 Manage Security Services

At this stage we will analyze minimizing the business impact of operational information vulnerabilities and defects, with a description of the process is to protect company information to maintain the level of information security risks that can be accepted by the company in accordance with security policies. Establish and maintain the role of information security and access rights and conduct security monitoring. The expected process capability model of DSS05 managing security services is level 4, a predictable process. In more detail are subdomains, see Table X. Ability to process DSS05 domains manage security services. It was concluded that the average DSS05 was at level 2.7, Managed Process.

TABLE X

DSS05 PROCESS CAPABILITY DOMAIN MANAGE SECURITY SERVICES

#	Sub Domain	Current	Expected
DSS05.01	Protect againts malware	3	4
DSS05.02	Manage network and connectivity security	3	4
DSS05.03	Manage endpoint security	3	4
DSS05.04	manage user identity and logical access	3	4
DSS05.05	Manage physical access to IT	3	4
DSS05.06	Manage sensitive documents and output devices	2	4
DSS05.07	Monitor the infrastructure for security-related events	2	4
Average		2.7	4

6) DSS06 Manage Business Process Controls

At this stage we will analyze to maintain the information integrity and security of information assets handled in business processes in the company or abroad, with a description of the process of defining and maintaining control of appropriate business processes to ensure that

information relating to and processed by in-house or outsourcing business processes fulfill all relevant information control requirements. Identify relevant information control requirements and manage and operate adequate controls to ensure that information and information processing meets these requirements. The expected process capability model DSS06 manages business process control is level 4, a predictable process. In more detail are the subdomains, see Table XI. The ability of the process DSS06 manages the control of business processes. Concludes DSS06 on average at level 2.2, Managed Process.

TABLE XI

DSS06 PROCESS CAPABILITY DOMAIN MANAGE BUSINESS PROCESS CONTROLS

#	Sub Domain	Current	Expected
DSS06.01	Align control activities embedded in business process with enterprise objectives	2	4
DSS06.02	Control the proessing of information	2	4
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority	2	4
DSS06.04	Manage errors and exceptions	3	4
DSS06.05	Ensure traceability of information events and accountabilities	2	4
DSS06.06	Secure informaton risk	2	4
Average		2.2	4

Fig. 5, Fig. 6 and Table XII. Pointing the level of capability processes of the entire process of the domain of Delivery, Service, and Support

TABLE XII

CONCLUSION OF DOMAINS OF DELIVER, SERVICE, AND SUPPORT

Average Domain	Current	Expected	Optimized
DSS01	2.8	4	5
DSS02	2.3	4	5
DSS03	2.4	4	5
DSS04	2.5	4	5
DSS05	2.7	4	5
DSS06	2.2	4	5

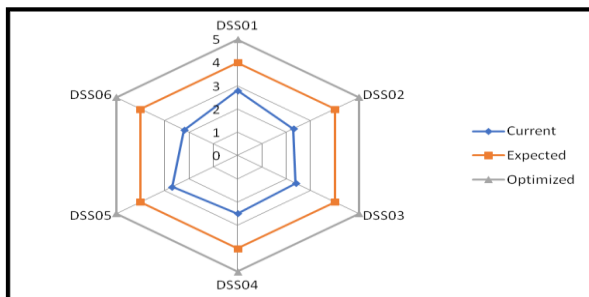


Fig. 5. Radar Graph of Process Capability Domain at Deliver, Service, and Support

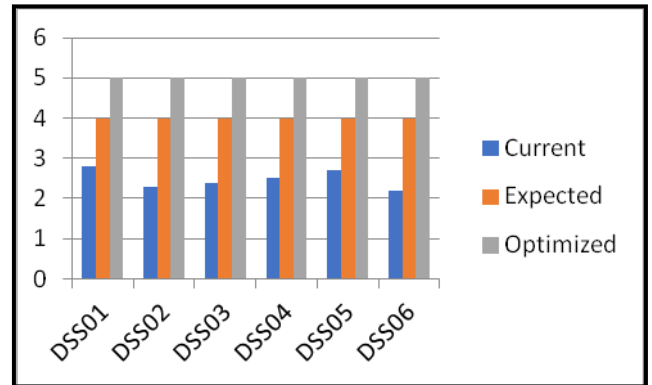


Fig. 6. Column Graph of Process Capability Domain Deliver, Service and Support

V. CONCLUSION AND FUTURE WORK

Based on the results of the analysis that has been done, it can be taken some conclusions related to the service information system at the Hospital, namely: IT governance in hospital services that have been carried out, although it is still not optimal because it has not reached the level of maturity that is expected to become the process capability model in each IT process contained. In the Deliver, Service, and Support (DSS) domains the average is 2.2 to 2.8 (managed process), and the IT governance process in hospital services has a pattern that is repeatedly performed.

In this study the author only focuses on the information system audit, it is expected that in the process of further research carried out with a broader scope, namely the audit of information technology governance. It is expected that in the next process of research can use the audit model other than COBIT 5 because COBIT only focuses on control and measurement. In addition, COBIT only provides control guidelines and does not provide guidance on operational implementation.

REFERENCES

- [1] Permenkominfo, "Peraturan Menteri No. 41 Tahun 2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional." Jakarta, 2007.
- [2] Sultani, "Pengembangan aplikasi audit sistem informasi berdasarkan," vol. 2012, no. Semantik, pp. 514–520, 2012.
- [3] D. Citha Astikasari and S. Elly Chandra, "Evaluation of Information Technology Governance with COBIT 5 in XYZ for ISO 27001:2013 Readiness," *International Journal of Engineering and Techniques*, vol. 4, no. 4, pp. 76–86, 2018.
- [4] A. Nuratmojo, E. Darwiyanto, S. T. Mt, G. Agung, A. Wisudiawan, and S. Kom, "Penerapan Cobit 5 Domain DSS (Deliver , Service , Support) untuk Audit Infrastruktur Teknologi Informasi FMS PT Grand Indonesia," *e-Proceeding of Engineering*, vol. 2, no. 2, pp. 6499–6506, 2015.
- [5] A. A. Yulius Budi Wijayanto, Bambang Soedijono W, "Audit Tata Kelola Teknologi Informasi Rumah Sakit Menggunakan Framework Cobit 5 (Studi Kasus di Rumah Sakit Panti Rapih)," vol. 10, no. 2, pp. 33–44, 2018.
- [6] R. Meadow, *A Business Framework for the Governance and Management of Enterprise IT*. 2012.