IT GOVERNANCE EVALUATION USING COBIT 5 FRAMEWORK ON THE NATIONAL LIBRARY

Ari Kurnia Setiawan, Johanes Fernandes Andry

Department of Information System, Faculty of Technology and Design, Universitas Bunda Mulia, Jl. Lodan Raya No. 2, Jakarta, 14430, Indonesia

Email: arikurnia1899@gmail.com, jandry@bundamulia.ac.id

Abstract

National Library of Indonesia (NLI) is a public library located in Jakarta, established by the decree of Ministry of Education and Culture in 1980. This day NLI has already applied digitalization of its contents and its management with IT, IT has been an important aspect in an organization. The objective of IT implementation is to increase effectivity and performance in organization. In order to get maximum results, good IT Governance is important in order to get good alignment between the IT and the business, the better IT Governance the greater outcome that the organization will get. This research will use qualitative method using COBIT 5 framework, interview and observation as research instruments, the reason of these method usage because authors can collect data as accurate as possible based on the actual condition. The objective of this research is to get an overview about the level of IT Governance on going, the analysis tool will be used is COBIT 5 focusing on DSS domain. The average score of DSS01, DSS02 and DSS03 is in 1.2 to 1.6 and for the DSS04, DSS05 and DSS06 domain the average score is between 2.1 and 2.3.

Keywords: *National Library of Indonesia, IT Governance, COBIT 5*

Abstrak

Perpustakaan Nasional Republik Indonesia (NLI) adalah perpustakaan publik yang terletak di Jakarta yang didirikan pada tahun 1980, berdasarkan keputusan dari kementrian pendidikan dan kebudayaan. Saat ini dalam operasionalnya NLI telah menerapkan digitalisasi konten-konten dan pengelolaannya dengan menerapkan Teknologi Informasi (TI). TI telah menjadi aspek penting dalam suatu organisasi, tujuan dalam penerapan TI adalah untuk meningkatkan keefektifan dan meningkatkan kinerja dalam suatu organisasi. Namun demi mendapatkan hasil yang maksimal IT Governance (tata kelola TI) yang baik sangatlah diperlukan dalam rangka menyelaraskan TI dengan bisnis, semakin baiknya IT Governance maka hasilnya yang didapat organisasi akan semakin maksimal. Metode yang digunakan dalam penelitian ini adalah metode kualtitatif menggunakan kerangka kerja COBIT 5, instrumen yang digunakan adalah observasi dan wawancara, alasan dipilihnya metode ini adalah agar penulis dapat mengumpulkan data seakurat mungkin sesuai dengan kondisi yang ada. Penelitian ini bertujuan untuk mendapatkan gambaran tentang tata kelola teknologi informasi yang sedang berjalan, alat analisis yang digunakan adalah COBIT 5 berfokus pada domain DSS. Hasil rata-rata yang didapatkan adalah domain DSS01, DSS02 dan DSS03 mimiliki rata-rata antara 1.2 sampai 1.6 dan untuk domain DSS04, DSS05 dan DSS06 memiliki rata-rata antara 2.1 sampai 2.3.

Kata Kunci: Perpustakaan Nasional Republik Indonesia, *IT Governance, COBIT 5*

1. Introduction

Library is an organization whose aim is to build and maintain knowledge and collection to provide information for research, educational, cultural etc. [1]. Public library is a center of information and knowledge, public library can be accessed by any users regardless their race, age, sex religion, language or social status. The public library is free of charge as the public library is the responsibility of the local governments. Its funding and operation must be supported and financed by local governments [2].

National Library of Indonesia (NLI) is a non-ministry government institution located at Gambir, south side of Merdeka Square, Jakarta. The national library was established in 1980 by the decree of Ministry of Education and Culture [3]. One of the NLI mission is to develop a modern national library infrastructure, modern library means that most of the content will be digitalized and can be accessed widely through the internet. In order to provide maximum service, effective and efficient IT governance is mandatory. Good IT governance ensure that the IT sustain and extends the NLI strategy and goals [4] [5].

In this era the needs for Information Technology is high because IT offers efficiency and effectiveness to support organization in achieving it goals. and because of the benefits many organizations make huge investments in IT [6] [7]. The success of IT implementation depends on the how well organization manages and monitor the IT, these action is to ensure that the IT implementation will generates benefits for the organization [8]. Poor management and monitoring can lead organization's IT investments will go in vain [9], In order to get maximum benefits from the IT investments organization must evaluate its IT Governance periodically.

This action is needed to oversee that the IT management is running well and optimum.

Organizations should adopt and implement IT Governance as its implementation is useful to ensure that the IT supports and aligns consistenly with the organizations objectives [5]. IT Governance concerns on how the IT in the organization is managed and structured, it provides practices that enable the alignment between business and IT to enhance their performance and governance [10] [11] [12]. COBIT (Control Objectives for Information and related Technology) is a framework developed and published by ISACA (Information Systems Audit and Control Association). COBIT has proven it reliability and has become worldwide leader in IT Governance, control security and assurance [13].

In this research authors will try to evaluate IT governance in NLI, the purpose of this research is to get an overview of the IT governance and performance in order to determine the capability levels of IT governance in NLI. COBIT 5 will be used as a guidance in assessing all processes within the IT function [14]. COBIT 5 helps the organization to create an optimal IT value by creating and maintaining the balance between benefits, optimizing the level of the risk and achieving goals through effective IT governance and IT management [14]. The domain that will be used in this research is Deliver, Service and Support, DSS focuses on delivery aspects of IT and support process that enables effective and efficient execution of IT.

2. Literature Review

IT Governance

Governance in business context is a series of rules, processes and actions that organization undertakes to determine organization strategies and operate the organization in a determined manner to help organization achieve it goals. While IT Governance refers to organizational structures and processes to ensure that the organization's IT fully support the organization goals [4] [15] [16].

IT Governance Institute (ITGI) defines that IT Governance can be applied into almost all kind of organizations, including aligning IT strategies with organization's strategies. Efficient IT resource allocation can help the organization to achieve its goals and in addition organization can carry out performance measurements to get an overview and assess how far the organizations has fulfilled their goals [15] [17]. The IT Governance definition can be seen on Figure 1. IT Governance Definition.

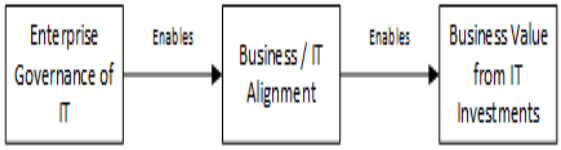

Figure 1. IT Governance Definition [13]

COBIT 5

COBIT (Control Objectives for Information and related Technology) is a set of documentation and guidelines for implementation of IT Governance. COBIT is a framework that helps auditors. Management and users to bridge the gap between business risk, needs, control and technical issues [15-16]. COBIT has experienced the evolution that is long enough to create best framework that can be used in implementation of the Enterprise IT Governance [18] [19].

COBIT 5 is a framework developed and published by ISACA (Information Systems Audit and Control Association) on 2012 [20]. It provides guidance for organizations in order to achieve organization's goals related to IT Governance and IT management. COBIT 5 provides comprehensive framework to support the establishment for an alignment between IT with the business itself. COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire organization, it covers the overall business process and functional areas of responsibility and considering the IT related interests of internal or external stakeholders [21] [22].

COBIT 5 allows organization to develop system and procedures for good IT control and management, the development is useful to provide management of Enterprise IT. COBIT 5 includes a set of 37 divided into two main processes shown in Figure 2 Governance and Management Key Areas.

Governance Processes

Governance processes is to ensure that enterprise objectives are optimally achieved by evaluating stakeholder needs, condition, option and set the direction through prioritization and monitoring the performance against agreed sets of goals.

Management Processes

Management processes is to manage plans, builds, runs and monitors working to ensure that the process set by the governance body will achieve the organizations objectives [24].

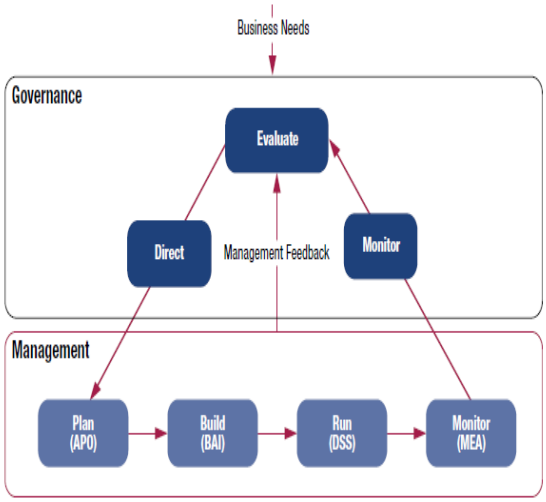

Figure 2. Governance and Management Key Areas [23]

3. Methods

This research is conducted by using qualitative method, the research instruments chosen are interview and observation because these instruments allows authors to gather and collect data simultaneously within the current situation [25]. The research flowchart can be seen on Figure 3 Research Flowchart.

Data from the observation were gathered by interviewing respondents, there are 3 respondents in total. the first one is the head of automation sub-field, the second and the third are the computer institution expert. Based on Figure 4 is the Interview Flowchart.

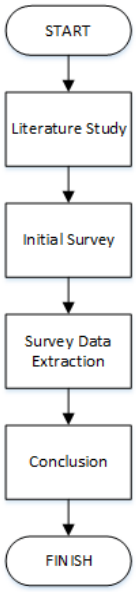

Figure 3. Research Flowchart [7]

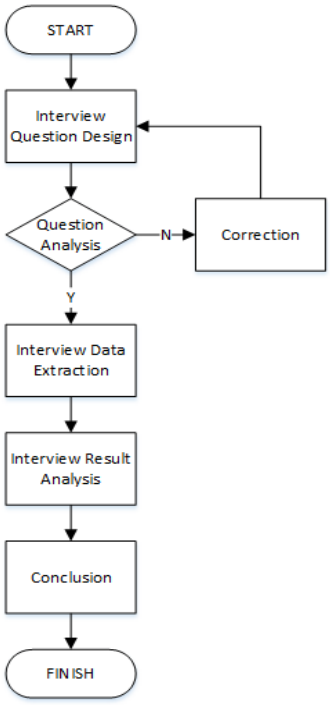

Figure 4. Interview Flowchart [7]

Report as the final result from the observation and interview is processed and calculated based on COBIT 5 capability levels model as seen on Table 1 COBIT 5 Capability Levels Model. The result will contain current capability level and expected capability level, after the calculation the next step is to do gap analysis in order to analyze the interpretation of the current and expected level and to provide recommendation and corrective action needed to overcome the gap and to achieve improvements in IT Governance.

TABLE 1
COBIT 5 CAPABILITY LEVELS MODEL [26]

Level	Description
Level 0: Incomplete	The process is not implemented or fails to achieve its purpose. At this level there is little or no evidence of any systematic achievement of the purpose.
Level 1: Performed	The implemented process already achieved its purpose. This process has one process attribute that is Process Performance.
Level 2: Managed	The performed process is now implemented and managed (planned, monitored and adjusted). This process has two process attributes that are Performance Management and Work Product Management.
Level 3: Established	The managed process is now implemented in a defined process that is capable of achieving its process outcomes. This process has two process attributes that are Process Definition and Process Deployment.
Level 4: Predictable	The established process now operates within defined limits to achieve its process

Level	Description
	outcomes. This process has two process attributes that are Process Management and Process Control.
Level 5: Optimizing	The predictable process is now continuously improved to meet relevant current and projected business goals. This process has two process attributes that are Process Innovation and Process Optimization.

4. Result and Analysis

In this step authors analyze the overall process with the COBIT 5 framework. Our analysis will be focusing on the IT department at the National Library of Indonesia (NLI). the analysis will include its employees, equipment, standard operational procedure etc. The domain that will be used in this process is Delivery, Service and Support (DSS).

DSS01 Manage Operations

The purpose of this sub-domain is to assess the coordination and the execution of the activities including the operational procedures that are important and required for the optimum delivery of internal and outsourced IT services. This sub-domain also includes the execution of pre-defined standard operating procedures and the required monitoring activities.

Most of the operations at the NLI is already running well, and the IT facilities are already being taken care and treated well. But there are lack of documentation to support the operations, the average score for this sub-domain is 1.2. the details of this sub-domain can be seen on table 2 Capability Levels of DSS01 Manage Operations.

TABLE 2
CAPABILITY LEVELS OF DSS01 MANAGE OPERATIONS

No.	Sub Domain	Current	Expected
DSS01.01	Perform Operational Procedures	1	3
DSS01.02	Manage Outsourced IT Services	1	3
DSS01.03	Monitor IT Infrastructure	1	3
DSS01.04	Manage the Environment	1	3
DSS01.05	Manage Facilities	2	3

DSS02 Manage Service Requests and Incidents

TABLE 3
CAPABILITY LEVELS OF DSS02 MANAGE SERVICE REQUESTS AND INCIDENTS

No.	Sub Domain	Current	Expected
DSS02.01	Define Incident & Service Requests Classification Schemes	1	3
DSS02.02	Record, Classify and Prioritize Requests and Incidents	1	3
DSS02.03	Verify, Approve and Fulfil Service Requests	2	3
DSS02.04	Investigate, Diagnose and Allocate Incidents	2	3
DSS02.05	Resolve and Recover from Incidents	2	3
DSS02.06	Close Service Requests and Incidents	0	3
DSS02.07	Track Status and Produce Reports	1	3

The purpose of this sub-domain is to assess the timeliness and effectiveness of the response given based on the user requests and resolution of all types of incidents, in order to increase productivity and minimize disruptions through quick resolution for the incidents.

Identification of user needs and recovery activities are already existing, all of the incident is already solved and already handled by experts in their field, reports is already being generated in timely manner and online reporting is already being implemented. But there is still no incident definition, escalation analysis and documentation about the incident. The average score for this sub-domain is 1.3. The details of this sub-domain can be seen on table 3 Capability Levels of DSS02 Manage Service Requests and Incidents.

DSS03 Manage Problems

The main purpose of this sub-domain is to assess the identification, classification of incidents and their root cause in order to provide best resolution in timely manner to prevent the incidents reoccur, also to enhance improvements from the recommendations composed in this sub-domain. the objective of this sub-domain are improvement of service levels, costs reduction and improvement of service by reduction the number of operational problems.

Identification of incidents are already done, known-error and its solutions are already made, problem, costs monitoring and progress reports for communication is already being implemented

supported by meetings to discuss occurring problems and upcoming problems. But there is still no IT service desk and system to support the recording and problem management. The average score for this sub-domain is 1.6. The details of this sub-domain can be seen on table 4 Capability Levels of DSS03 Manage Problems.

TABLE 4
CAPABILITY LEVELS OF DSS03 MANAGE PROBLEMS

No.	Sub Domain	Current	Expected
DSS03.01	Identify & Classify Problems	1	3
DSS03.02	Investigate & Diagnose Problems	1	3
DSS03.03	Raise Known Errors	3	3
DSS03.04	Resolve and Close Problems	1	3
DSS03.05	Perform Proactive Problem Management	2	3

DSS04 Manage Continuity

The purpose of this sub-domain is to assess the establishment and the maintenance of a plan that will enable the business and IT respond to an incident in a harmony and in timely manner, this action purpose is to ensure the operation of critical business process and required IT services goes well when incidents occurring, also to maintain the availability of information when incidents ocurring. The objective of this sub-domain is to continue critical business operations and maintain, provide availability of data & information in the event of a disruption.

Identification of internal, outsourced service, key stakeholder, business process and scenario is already done. Backup of data is already done regularly. Business analysis is already implemented and business continuity plan and the response is also already being made supported by regular review, maintenance and improvement of the continuity plan. But the Business Continuity Plan (BCP) hasn't tested yet, so the training and its review could not be done. The average score for this sub-domain is 2.1. The details of this sub-domain can be seen on table 5 Capability Levels of DSS04 Manage Continuity.

TABLE 5
CAPABILITY LEVELS OF DSS04 MANAGE CONTINUITY

No.	Sub Domain	Current	Expected
DSS04.01	Define the BCP, Objectives & Scope	3	3
DSS04.02	Maintain a Continuity Strategy	3	3
DSS04.03	Develop and Implement a Business Continuity Response	3	3
DSS04.04	Exercise, Test & Review BCP	0	3
DSS04.05	Review, Maintain & Improved the Continuity Plan	2	3
DSS04.06	Conduct Continuity Plan Training	2	3
DSS04.07	Manage Backup Arrangements	3	3
DSS04.08	Conduct Post-resumption Review	1	3

DSS05 Manage Security Services

The purpose of this sub-domain is to assess the protection of organization information in order to maintain the information security according to the security policy, and the establishment alongside with the maintenance of IT security roles, access privileges and performance of security monitoring.

Every policy is already made based on the risk and business evaluation there is already activities to protect devices against malware and the software used is already updated regularly. Network security and its protocol already exist and network filtering is already implemented, endpoint devices is already managed and configured well. Management of user identity, logical access, management of sensitive documents and outputs device alongside with physical access management is already managed well. But the anti-malware software distribution is still done manually and there is no security events review, internal or external audit to audit the access of sensitive information is still not implemented. The average score for this sub-domain is 2.1. The details of this sub-domain can be seen on table 6 Capability Levels of DSS05 Manage Security Services.

TABLE 6
CAPABILITY LEVELS OF DSS05 MANAGE SECURITY SERVICES

No.	Sub Domain	Current	Expected
DSS05.01	Protect Against Malware	1	3

No.	Sub Domain	Current	Expected
DSS05.02	Manage Network and Connectivity Security	2	3
DSS05.03	Manage Endpoint Security	2	3
DSS05.04	Manage User Identity & Logical Access	3	3
DSS05.05	Manage Physical Access to IT Assets	3	3
DSS05.06	Manage Sensitive Documents & Output Devices	3	3
DSS05.07	Monitor the Infrastructure for Security Related-Events	1	3

DSS06 Manage Business Process Controls

The purpose of this sub-domain is to assess the definition and maintenance of business process controls to ensure the information needed satisfies all relevant control requirement. The objective of this sub-domain is to maintain information integrity and security within business process either processed internally or outsourced.

TABLE 7
CAPABILITY LEVELS OF DSS06 MANAGE BUSINESS PROCESS CONTROLS

No.	Sub Domain	Current	Expected
DSS06.01	Align Control Activities Embedded in Business Processes with Enterprise Objectives	2	3
DSS06.02	Control the Processing Information	3	3
DSS06.03	Manage Roles, Responsibilities, Access Privileges and Levels of Authority	2	3
DSS06.04	Manage Errors & Exceptions	2	3
DSS06.05	Ensure Traceability of Information Events & Accountabilities	2	3
DSS06.06	Secure Information Assets	3	3

There is already identification and documentation done about control activity, monitoring is already implemented to enhance improvement. Every information transaction is made according to procedure and its verified to ensure its accuracy, information asset is already classified and training is already conducted alongside with good security, error correction procedure and review. But access control is still not reviewed periodically. The average score for this sub-domain is 2.3. The details of this sub-domain can be seen on table 7 Capability Levels of DSS06 Manage Business Process Control.

Based on the research conducted, improvements is needed in order to improve the performance level that are below the expected level. these are the recommendations for the improvements are:

Recommendation based on DSS01 Manage Operations

In this domain, lack of documentation is the major problem. Definition and documentation is still not done thoroughly, NLI should document and define all of the SOP so all of the activity is well documented and can be monitored or revised periodically.

Recommendation based on DSS02 Manage Service Requests and Incidents

These domains, lack of definition, documentation and escalation analysis are the major problem. Definition and documentation is still not done thoroughly, NLI should document and define all of the SOP so all of the activity is well documented and can be monitored or revised periodically. NLI should also do escalation analysis, escalation analysis useful to keep track of the problem that frequently occur. the analysis also can be used for the reference to produce solutions for the problems.

Recommendation based on DSS03 Manage Problems

In this domain the major problem is there is no IT service desk and the system. NLI should implement IT service desk and system, this implementation is needed to create incidents ticket, incidents recording and incidents progress monitoring.

Recommendation based on DSS04 Manage Continuity

In this domain the major problem is the BCP is never tested, trained or reviewed. NLI should test, train and review the BCP regularly, this actions is needed in order to improve, maximize and to detect flaws from the BCP and to provide the corrections needed.

Recommendation based on DSS05 Manage Security Services

In this domain the major problem are anti-malware software distribution is still done manually, no security events review and internal audit on sensitive information is still not conducted. NLI should distribute anti-malware software centrally so all of the anti-malware software on devices can be installed and updated at the same time. NLI also should review security events regularly in order to make sure there is no severe security events occurring without the NLI knowledge. NLI should also conduct internal audit on sensitive information regularly, this action is needed to prevent sensitive information accessed by unwanted party.

Recommendation based on DSS06 Manage Business Process Controls

These domains the major problem is access control is still not reviewed periodically, NLI should do this action in order to prevent unauthorized user can modify or access sensitive information.

TABLE 8
SUMMARY OF PERFORMANCE LEVEL ON DSS DOMAIN

No.	Current	Expected
DSS01 Manage Operations	1.2	3
DSS02 Manage Service Requests & Incident	1.3	3
DSS03 Manage Problems	1.6	3
DSS04 Manage Continuity	2.1	3
DSS05 Manage Security Services	2.1	3
DSS06 Manage Business Process Controls	2.3	3

The summary of the performance level can be seen on table 8 summary of performance level on DSS domain and figure 5 Radar chart of the Summary of the Performance Level on DSS Domain.

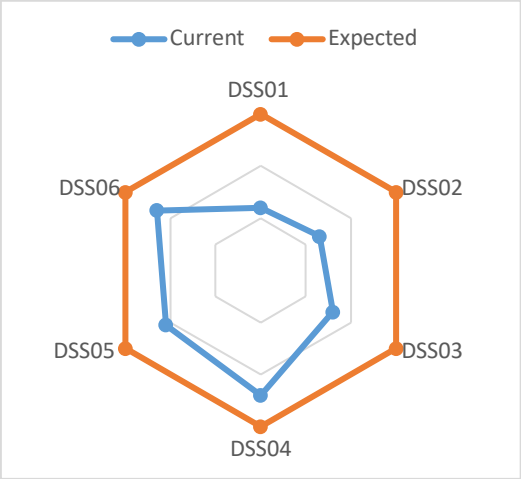

Figure 5. Radar chart of the Summary of Performance Level on DSS Domain

5. Conclusion

The conclusion of this research is that the IT governance at the NLI has already implemented but most of them still not run optimally because they have not reached the expected level.
on DSS01 manage operations the average score is 1.2, on DSS02 manage service requests and incident the average score is 1.3, on DSS03 manage problems the average score is 1.6, on DSS04 manage continuity the average score is 2.3, on DSS05 manage security services the average score is 2.1, on DSS06 manage business process controls the average score is 2.3.

The performance level of DSS01, DSS02 and DSS03, they are still at level 1 performed process, on the DSS04, DSS05 and DSS06 the performance level is still at level 2 managed process. Result of this research is the performance of IT Governance in NLI has already performed, but most of it is still not defined, formalized and documented. We hope this research and recommendations can be used by NLI as reference for the improvement of their IT Governance.

References

[1] UNESCO, 1 January 2019. [Online]. Available: http://uis.unesco.org/en/glossary-term/library. [Accessed 24 January 2019].

[2] International. Federation. of. Library. Associations, 1 Jauary 2019. [Online]. Available: https://www.ifla.org/publications/iflaunesco-public-library-manifesto-1994. [Accessed 24 January 2019].

[3] The. National. Library. of. Indonesia,

Country Report Conference of Directors of National Libraries – Asia & Oceania (CDNL-AO), 2008.

[4] J. F. Andry and K. Christianto, Audit menggunakan COBIT 4.1 dan COBIT 5 dengan Case Study, Teknosain, 2018.

[5] C. Marnewick and L. Labuschagne, "an Investigation Into Governance of Information Technology Projects in South Africa," *International Journal of Project Management,* vol. 29, no. 6, pp. 661-670, 2011.

[6] Tridoyo and A. F. Wijaya, "Analysis of Information Technology Governance e-KTP using COBIT 5 Framework," *International Conference on Innovative and Creative Information Technology (ICITech),* pp. 1-6, 2017.

[7] J. F. Andry, "Performance Measurement of Information Technology Governance: a Study Case," *Jurnal Sistem Informasi (Journal of Information Systems),* vol. 2, no. 12, pp. 56-62, 2016.

[8] D. H. Steven and V. G. Wim, Enterprise Governance of Information Technology: Achieving Alignment and Value Featuring COBIT 5, Springer, 2015.

[9] I. K. Nisrina, I. J. M. Edward and W. Shalannanda, "IT Governance Framework Planning Based on COBIT 5 Case Study: Secured Internet Service Provider Company," *2nd International Conference on Wireless and Telematics (ICWT),* pp. 51-56, 2016.

[10] M. R. F. V. A. Garzoni, "The impact of an IT Governance Framework on the Internal Control," *Records Management Journal,* vol. 27, no. 1, pp. 19-41, 2017.

[11] S. D. H. W. V. Grembergen and R. S. Debreceny, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *Journal of Information Systems,* vol. 27, no. 1, pp. 307-324, 2013.

[12] E. N. Nfuka and L. Rusu, "The Effect of Critical Success Factors on IT Governance Performance," *Industrial Management & Data Systems,* vol. 111, no. 9, pp. 1418-1448, 2011.

[13] A. Pasquini and E. Galiè, "COBIT 5 and the Process Capability Model Improvements Provided for IT Governance Process," *Proceedings of FIKUSZ '13 Symposium for Young Researchers,* pp. 67-76, 2013.

[14] ISACA, "COBIT 5: Enabling Process," 2012.

[15] D. G. Stephen, The Basics of IT Audit, Syngress, 2013.

[16] T. Sethibe, J. Campbell and C. McDonald, "IT Governance in Public and Private Sector Organisations: Examining the Differences and Defining Future Research Directions," *18th Australasian Conference on Information Systems,* pp. 833-843, 2007.

[17] IT. Governance. Institute, "Board Briefing on IT Governance," Rolling Meadows, 2003.

[18] K. R. P. Harefa and N. Legowo, "The Governance Measurement of Information System Using Framework COBIT 5 in Automotive Company," *International Conference on Applied Computer and Communication Technologies (ComCom),* 2017.

[19] IT. Governance. Institute, *Steering Comittee,* 2012.

[20] L. Maseko and B. Marx, "An Analysis of COBIT 5 as a Framework for the Implementation of IT Governance with Reference to KING III," *Risk governance & control: financial markets & institutions /,* vol. 6, no. 1, pp. 20-34, 2016.

[21] S. Ahriz, K. M. Abir El Yamami and M. Qbadou, "Cobit 5-Based Approach for IT Project Portfolio Management: Application to a Moroccan University," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 9, no. 4, pp. 88-95, 2018.

[22] S. Ramloui and A. Semma, "Comparative Study of COBIT with other IT Governance Frameworks," *IJCSI International Journal of Computer Science Issues,* vol. 6, no. 1, pp. 95-101, 2014.

[23] ISACA, "COBIT 5: a Business Framework for the Governance and Management of Enterprise IT," 2012.

[24] ISACA, "COBIT 5 Executive Summary," 2012.

[25] A. Queirós, D. Faria and F. Almeida, "Strengths and Limitations of Qualitative and Quantitative Research Methods," *European Journal of Education Studies,* vol. 3, no. 9, pp. 369-387, 2017.

[26] ISACA, "Self-assessment Guide: Using COBIT 5," 2012.