



Available online to www.journal.unipdu.ac.id

Unipdu

S2-Accredited – SK No. 34/E/KPT/2018

Journal page is available to www.journal.unipdu.ac.id:8080/index.php/register



IT governance evaluation at the population and civil registry office in Kolaka district using COBIT 5 framework

Noorhasanah Zainuddin ^a, Wing Wahyu Winarno ^b, Nurfitriani Ningsi ^c, Yuwanda Purnamasari Pasrun ^d, Muliyadi Muliyadi ^e

^{a,c,d,e} Department of Information Systems, Universitas Sembilanbelas November Kolaka, Kolaka, Indonesia

^b Department of Accounting, Sekolah Tinggi Ilmu Ekonomi YKPN, Yogyakarta, Indonesia

email: ^a Noorhasanahzain@gmail.com

ARTICLE INFO

Article history:

Received 27 October 2019
Revised 21 May 2020
Accepted 22 May 2020
Published 14 June 2020

Keywords:

COBIT 5
Disdukcapil
DSS
IT Governance
Process Assessment Model

IEEE style in citing this article:

N. Zainuddin, W. W. Winarno, N. Ningsi, Y. P. Pasrun and M. Muliyadi, "IT governance evaluation at the population and civil registry office in Kolaka district using COBIT 5 framework," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 86-95, 2020.

ABSTRACT

The implementation of information technology is compulsory to fit organizational goals. This research aims to evaluate the quality of information technology services at the Population and Civil Registry Office at Kolaka District based on COBIT 5 Framework that focused on DSS (deliver, service and support) domain by measuring the Maturity Level using Process Assessment Model (PAM). The Population and Civil Registry Office is under the local government 's auspices which is essential in managing the population. The data collection method was done by distributing questionnaires and conducting interviews. This study used 8 (eight) respondents based on the RACI chart. This research was expected to reach level 3 (established process) to create IT governance that fits organizational goals and international standards. From the research result, it is known that the maturity level from the evaluation process conducted by COBIT 5 using the processes DSS-01, DSS-02, DSS-03, DSS-04, DSS-05, and DSS-06 were as follows: 2 processes were at level 1 (performed process), namely the DSS-05 and DSS-06 while the others (DSS-01, DSS-02, DSS-03, and DSS-04) were at level 2 (managed process).

2020 Register: *Jurnal Ilmiah Teknologi Sistem Informasi* (Scientific Journal of Information System Technology) with CC BY NC SA license.

1. Introduction

In this era, the need for Information Technology (IT) is quite high because it offers efficiency and effectiveness to support the organization in achieving its goals. Due to its' benefits, many organizations make huge investments in IT [1]. The existence of IT is realized by companies because it can contribute to the improvement of their competitiveness. The benefits of IT are also enjoyed by various levels of business, society, and government [2, 3]. Institutional goals will be achieved if information technology planning and strategies are implemented following the organization's business planning and strategy [4]. The user's changing need also affects the use of technology in the future [5]. Therefore, information technology governance is effective when IT managers can integrate IT planning and organization to achieve a match between the dynamics of the business environment and governance desired by the board [6].

The Population and Civil Registry Office, abbreviated into DISDUKCAPIL, is one of the services under the local government's auspices. One of the DISDUKCAPIL missions is to give smooth, fast, precise, and transparent population and civil registration services to realize excellent services.

DISDUKCAPIL has implemented a Population Administration Information System (SIAM) to support its operations. In order that the DISDUKCAPIL can do IT operational services and timely services, it must be in optimal conditions. DISDUKCAPIL has never evaluated IT governance externally. For this reason, it is necessary to measure the maturity level of DISDUKCAPIL information technology governance services. Conducting an IT governance evaluation process can give information on the quality of IT development and its implementation.

The framework used is Control Objective for Information and Related Technology (COBIT) 5 developed by the IT Governance Institution, which is part of (ISACA), consisting of best practices guidance. It presents the IT organization activities in manageable and logical structure, compiled by experts in the IT governance field, and focuses more on control, not on execution. This framework helps organizations to optimize IT investment, to ensure service delivery, and to provide a measurement of what can be done when an error occurs [7].

IT governance plays a vital role in enhancing IT capabilities [8]. Effective IT governance is one of the critical things that need to be possessed by policymakers. For business people, maximum investment in IT is a strategy to survive in a competitive market [7, 9].

COBIT provides a comprehensive framework service to help government and IT management. This framework has been widely used in previous studies to evaluate, audit, and design IT governance in general, focusing on several areas of IT governance. Some of these studies differ in the object of research and the process used.

Research conducted by Jarsa and Christianto [10] at PT. Andal Software company focused on issues of maintenance and custom or repair processes carried out by the company. The evaluation used was COBIT 5 on DSS 01, DSS 02, DSS 03, and DSS 06 domains showing the result on level 1.

Further research was conducted by J.F Andry using COBIT 5 to measure the IT governance level of achievement. Aspects that needed to be considered were efficiency, effectiveness, and functional IT units in the organization. The study showed that the average score was at 2.2 to 2.8 (managed process) [4]. Setiawan and Andry [11] conducted an audit using COBIT 5 and DSS domain focus. The DSS-01, DSS-02, and DSS-03 average score showed within 1.2 to 1.6, while for DSS-04, DSS-05 and DSS-06 was between 2.1 and 2.3. Astuti et al. [12] also used COBIT 5 as a framework to identify the IT processes. Risks were identified from the Service Desk's business processes and existing conditions of DPTSI. And then, they were mapped to corresponding ideal conditions based on COBIT 5 process DSS-02 manage service requests and incidents. Furthermore, risks related to information technology processes were identified using APO12 Manage Risks process.

Riki et al. [13] conducted a study focusing on the DSS domain, namely the IT process DSS-01 and DSS-03. The results of the study showed that the DSS-01 average value was 1.8, while the DSS-03 average valued was 2.2. Because this capability was still at a low level, improvements were still needed to reach the minimum requirements set by the company.

In this current research, the use of COBIT 5 Domain DSS was expected to be able to reach the expected level (level 3), so that local government services could create comprehensive alignment between business and IT that had been invested.

2. Literature Review

2.1. Evaluation and performance measurement

Performance is an actual work produced by a specific unit or entity, which refers to the measurable achievements produced. The term "measurement" points to the process used to provide a quantification of particular abilities, events, or activities [14].

The evaluation of a system was one of the crucial aspects needed to determine the success of an information system. The information will be obtained through the assessment of information systems to what extent the success of achieving the system's goals is. Evaluation is generally carried out with an audit process to measure the level of maturity and IT governance readiness of a company. To achieve IT service needs and company goals in terms of IT governance audits, framework COBIT 5 is one of the standard terms used [15].

2.2. Information technology governance

IT governance is a branch of governance that focuses on IT systems, performance, and risk management [16]. IT governance is an integral part of corporate governance, functions as an instrument that supports IT sustainability, and extends the organization's strategy and objectives [17]. The implementation of IT Governance was one of the biggest challenges for any organization to ensure that IT was fit with the business goals [11]. The primary goals of it government were to invest in the business value creation and risk reduction by implementing a well-defined organizational structure [18].

Information Technology Governance Institute (ITGI) defines that IT Governance can be applied to almost all kinds of organizations, including aligning IT strategies with the organization's policies. Efficient IT resource allocation can help the organization carry out performance measurements to get an overview and assess how far the organizations have met their goals [11]. The primary purpose of IT governance is to invest in the business value creation and risk reduction by implementing a well-defined organizational structure. The focus IT governance can be divided into 5 parts namely; strategic alignment, value delivery, risk management, resource management, performance measurement [7] as shown in Figure 1.



Figure 1. IT governance focus [7]

2.3. COBIT framework

COBIT is a collection of documentation and guidance that leads to IT governance. It can help auditors, managers, and users to bridge the gap between the business control model and the information technology control model [19]. COBIT was firstly developed in 1996 by the IT Governance Institute (ITGI), which was part of the Information Systems Audit and Control Association (ISACA). The most reliable framework, COBIT 5, is a service for auditing information systems quickly, accurately, and interactively [4].

The Cobit Framework is a collection of best practices for IT management, created by system auditing, assurance, and Information technology directives. There are three levels in COBIT. At the lowest level, there are activities and tasks required to achieve measurable results. At a higher level, the process is defined as the set of tasks and activities. Furthermore, at the highest level, the focus of attention is on processes that are grouped in 4 areas [18].

COBIT has experienced a long enough evolution to create the best framework for the implementation of IT governance in the enterprise [11]. COBIT 5 Framework provides a comprehensive framework to support establishment for alignment between IT and the business itself and allows information that related technology to be regulated and holistically managed for the whole organization [20, 21].

The use of the COBIT 5 framework for risk management was done by analyzing existing SLA by identifying gaps, followed by a producing template in which the identified gaps were addressed [22]. Besides, the effectiveness of COBIT 5 in the reduction of the risk of Cyber Attacks on SCMS (Supply Chain Management System) 18 was also performed [23].

2.4. Process model assessment

Process Assessment Model is based on COBIT 5, according to the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 15504. This model is the basis for evaluating an IT process's ability in an organization/company toward COBIT 5. The IT governance

framework plays a role in stimulating accountability and transparency by increasing IT information reports to external stakeholders, especially in conditions where the IT strategic role is very high [24]. The evaluation model allowed the assessment by companies to support the improvement process. Mapping was designed to determine the process to be assessed [25].

The assessment model (PAM) process is a measurement model used in Cobit 5. PAM in cobit 5 is divided into two parts, the first is the capability dimension which is a scale rating technique used to assess capability levels, the second is the dimension of the process of defining and classifying which consists of 5 dimensions of the EDM, APO, BAI, DSS and MEA [25].

With the maturity level model, the organization can comprehend the current position, and continuously increase its level to the highest level so that governance aspects of IT work effectively. The capability levels and process attributes above were shown in Table 1.

Table 1. Capability Level and Process Attribute [25]

Level	Capability	Process Attribute (PA)
0	Incomplete	
1	Performed	1.1.Performance
2	Managed	2.1.Performance management 2.2.Work product management
3	Established	3.1.Definition 3.2.Deployment
4	Predictable	4.1.Measurement 4.2.Control
5	Optimizing	5.1.Innovation 5.2.Optimization

2.5. Process reference model in COBIT 5

The Framework of COBIT 5 had five domains and 37 processes in which all domains had the same role in achieving the IT goals [7].

3. Research Method

This research used qualitative data in the form of interviews and supporting related literatures. Besides, it also used the questionnaire as quantitative by data using the Guttman Scale. The flow of this research can be seen in the following flowchart in Figure 2, consisting of 7 processes as follows:

1. A literature review was carried out by gathering literature consisting of documents and information related to this research.
2. The researchers determined the domain with six sub-domains, DSS-01, DSS-02, DSS-03, DSS-04, DSS-05, and DSS-06.
3. Identification of respondents using the RACI method (responsible, accountable, consulted, informed) chart was performed. The researchers determined eight respondents who possessed the roles and responsibilities in decision making and then mapped the COBIT 5 process.
4. The data collection method was carried out by distributing questionnaires and then conducting interviews to clarify the filling out of the questionnaire data and collecting evidence of process implementation documents.
5. Data processing was done by assessing a questionnaire and producing quantitative data, so it needed to be simplified, and presented in a systematic arrangement.
6. Data analysis techniques used descriptive arithmetic techniques to describe the research variables in measurement. Firstly the level of capability was determined using the PAM (process assessment model) method that produced a percentage. The percentage would later be the determinant in the rating scale, which was presented in the form of a frequency distribution table or in the form of a visual (pie chart) to determine the tendency of research findings, whether it was included in the low, medium, or high category. Recommendations obtained from the results of the analysis were to produce any processes that needed to be considered to improve the performance required by the organization.
7. At this stage, conclusions were drawn based on the results of interviews, analysis, and answer-

ed research questions. Furthermore, suggestions were given to be used as materials for improvement, consideration by the organization, and references for further research.

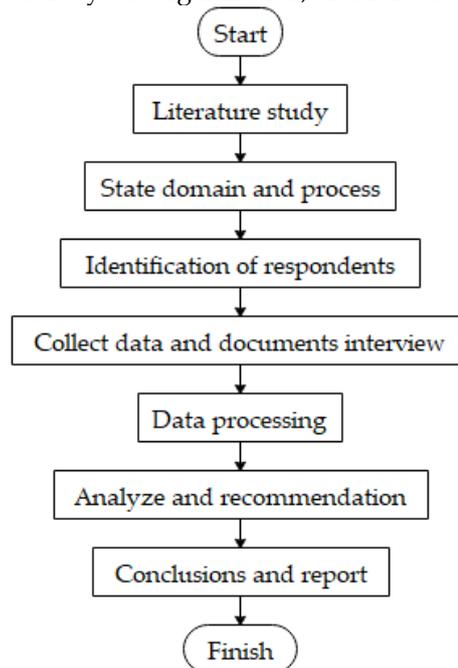


Figure 2. Research methodology

4. Experiment and Results

The first stage was conducted by gathering information and data needed in each process of the organization through interviews, observation, literary study, and questionnaire. All of the data and information obtained were formulated to solve the problem.

At this stage, the researchers identified the problem by using the COBIT 5 framework to determine the control objectives. This research was focused on the DSS domain (delivery, support, and system), which obtained 6 IT processes, namely; DSS-01, DSS-02, DSS-03, DSS-04, DSS-05, and DSS-06. The next step was to measure the maturity level of each attribute.

DSS-01 sub domain manage operations

This sub Domain aimed to assess the coordination of operational activities and procedures needed to provide services for internal and external parties, including the supervision and implementation of standard operational procedures. This process consisted of 5 sub-processes and 34 statements.

All of the DSS-01 sub-domains in the Population and Civil Registry Office in Kolaka District have been implemented well in a more orderly manner (planned, monitored, and adjusted), and the resulting product work has been well established, controlled, and maintained. The mean score on the DSS-01 sub-domain was 2.08. The details of this subdomain can be seen in Table 2.

Table 2. Capability levels of manage operation (DSS-01)

Domain	Process Name	Current Capability	Expected Capability
DSS-01.01	Perform Operational Procedures	2	3
DSS-01.02	Outsourced IT Services Management	2	3
DSS-01.03	IT Infrastructure Monitoring	2	3
DSS-01.04	Environment Management	2	3
DSS-01.05	Facilities Management	2.4	3

DSS-02 manage service requests and incidents

The purpose of this subdomain was to assess response timeliness and request effectiveness from users and the resolution of all types of incidents. Thus, it could increase productivity and minimize disruption; restore the service to normal; and resolve incidents. This process consisted of 7 sub-processes with 24 statements.

In the DSS-02 sub Domain, definitions of incident and classification of requests have been carried out well, identification of user needs and return of service recovery have been fulfilled, and all incidents

have been resolved and handled by experts in their fields. Regular and timely reporting, and online reporting, have been appropriately accomplished, resulting in a 2.07 average score on the DSS-02 sub-domain. The details of this sub-domain can be seen in Table 3.

Table 3. Capability levels of manage service request and incidents (DSS-02)

Domain	Process Name	Current Capability	Expected Capability
DSS-02.01	Define Incident & Service Requests Classification Schemes	2.5	3
DSS-02.02	Record, Classify, & Prioritize Requests & Incidents	2.2	3
DSS-02.03	Verify, Approve, & Fulfil Service Requests	2	3
DSS-02.04	Investigate, Diagnose, & Allocate Incidents	1.9	3
DSS-02.05	Resolve, & Recover from Incidents	1.9	3
DSS-02.06	Close Service Requests & Incidents	2	3
DSS-02.07	Track Status and Produce Reports	2	3

DSS-03 sub domain manage problems

The purpose of this Sub Domain was to assess the identification, classification and the root of the problem; to provide the best resolution promptly to prevent recurring events; and to provide recommendations to increase the improvement. Consequently, it could increase availability, improve service levels, reduce costs, increase customer comfort and satisfaction, and reduce operational problems. This process consisted of 5 sub-processes with 23 statements.

In the DSS-03 sub-domain, incident identification and classification, investigation and diagnosis of problems using experts in the field and sustainable solutions for the future have been implemented well. Lastly, the operational data collection and analysis have been made logs especially incident data and change data to activate the assessment that has been implemented. The average score on the DSS-03 sub-domain was 2. The details are shown in Table 4.

Table 4. Capability levels of manage problems (DSS-03)

Domain	Process Name	Current Capability	Expected Capability
DSS-03.01	Identify & Classify	2.2	3
DSS-03.02	Investigate & Diagnose	2	3
DSS-03.03	Raise Known Errors	2	3
DSS-03.04	Resolve & Close	1.8	3
DSS-03.05	Proactive Problem Management	2	3

DSS-04 manage continuity

The purpose of this Sub Domain was to assess the establishment and maintenance of plans so that IT can respond to the incidents and disruptions on time to continue the business process. This action aimed to ensure the critical business process and IT services as well as the availability of information at an acceptable level by the organization running well when the incident occurred. The process consisted of 8 sub-processes with 42 statements.

In the DSS-04 Sub-Domain, identifying scope, continuous strategy, and periodic review were available, but they were in the test sub-process. The BPC review was not been tested, so training and evaluation could not be carried out. The average score on the DSS-04 sub-domain was 2. The details can be seen in Table 5.

Table 5. Capability levels of manage continuity (DSS-04)

Domain	Process Name	Current Capability	Expected Capability
DSS-04.01	Define the BCP, Objectives & scope	2	3
DSS-04.02	Maintain a Continuity Strategy	2	3
DSS-04.03	Develop & Implement a Business Continuity Response	2	3
DSS-04.04	Exercise, Test & Review BCP	0	3
DSS-04.05	Review, Maintain & Improved the Continuity Plan	2	3
DSS-04.06	Conduct Continuity Plan Training	2	3
DSS-04.07	Manage Backup Arrangements	3	3
DSS-04.08	Conduct Postresumption Review	1	3

DSS-05 manage security service

This sub-domain aimed to assess the level of protection of information. The assessment was carried out to minimize security risks based on security policies, define and maintain the role of information security and access rights and accomplish security monitoring. This process consisted of 7 sub-processes with 49 statements.

Every policy in the DSS-05 sub-domain was made based on business risk evaluation and was prepared for the protection, prevention, and correction of the malware. Periodic updates, network security, and protocols were available. Endpoint devices have been implemented and well configured. User identity and logical access management, sensitive documents and output devices management, and monitor the infrastructure for security-related events had been applied properly, but they were not organized yet. The distribution of anti-malware software was still performed manually, with no security reviews were available.

The average score on the DSS-05 sub-domain was 1.1. The details of the DSS-05 sub-domain can be seen in Table 6.

Table 6. Capability levels of manage security service (DSS-05)

Domain	Process Name	Current Capability	Expected Capability
DSS-05.01	Malware Protection	1.2	3
DSS-05.02	Network & Connectivity Security Management	1.1	3
DSS-05.03	Endpoint Security Management	1	3
DSS-05.04	User Identity & Logical Access Management	1	3
DSS-05.05	Physical Access to IT Assets Management	1.2	3
DSS-05.06	Sensitive Documents & Output Devices Management	1.2	3
DSS-05.07	Monitor the Infrastructure for Security-Related Events	1	3

DSS-06 manage business process controls

This Sub-domain aimed to determine and maintain the appropriate business processes controls to ensure relevant information, whether processed by in-house or outsourced. This sub-domain identified control requirements, managed, and operated adequate information controls to ensure that information processing met the requirements. This process consisted of 6 sub-processes with 32 statements.

In this sub-domain, identification and documentation of the implementation of business process activities and related controls have been carried out by operating the implementation of business process activities to ensure their accuracy. The authority to access information assets have been allocated according to their roles and responsibilities, asset classification, error correction procedures, and the review. To add, training to use the system for staff also have been implemented. However, all of these carried out activities have not been controlled periodically. The average score on the DSS-06 sub-domain was 1.1. The details of the DSS-06 sub-domain can be seen in Table 7.

Table 7. Capability levels of manage business process controls (DSS-06)

Domain	Process Name	Current capability	Expected Capability
DSS-06.01	Align Control Activities Embedded in Business Processes with Enterprise Objectives	1	3
DSS-06.02	Control the Processing Information	1	3
DSS-06.03	Manage Roles, Responsibilities, Access Privileges and Levels of Authority	1.2	3
DSS-06.04	Manage Errors & Exceptions	1.2	3
DSS-06.05	Ensure Traceability of Information Events & Accountabilities	1	3
DSS-06.06	Secure Information Asses	1	3

Based on the results of this research, a revision was needed to improve the level of performance by the expected target. Recommendations for each DSS Sub Domain were as follows:

Recommendation on DSS-01 sub domain manage operations

The main problem in this sub-domain was the unavailability of process output lists required at level 3.

What was needed to do by DISDUKCAPIL was to record the quality and performance related to managing IT service operations.

Recommendation on the DSS-02 sub domain manage service requests and incidents

In this sub-domain, the main problems were the periodical recording of investigations, diagnoses, and allocations of incidents, these problems could make the quality and performance regarding Manage Service Requests and Incidents unknown. In this case, DISDUKCAPIL required the recording quality and recording performance related to Manage Service Requests and Incidents of IT services.

Recommendation on DSS-03 sub domain manage problems

In this sub-domain, the issue was in the unavailability of the process outputs that were required to reach level 3. Therefore, DISDUKCAPIL was suggested to record the quality and performance related to IT service problem management.

Recommendation on DSS-04 sub domain manage continuity

In this sub-domain, the main problem was that the BCP has never been tested, trained, or reviewed. So, DISDUKCAPIL was advised to conduct regular BCP training, testing, and review to detect, improve, and maximize BCP deficiencies and provide the quality and performance records related to managing Continuity of IT services.

Recommendation on the DSS-05 sub-domain manage security service

In this sub-domain, the main problem was the lack of documentation and SOP about managing security services. Thus, DISDUKCAPIL was advised to carry out routine, regular and periodic documentation and can be monitored or revised periodically.

Recommendation on DSS-06 sub domain manage business process controls

This sub-domain was focused on the lack of documentation and SOP. Definitions and documentation on a regular and periodic basis were not carried out. Therefore, DISDUKCAPIL was suggested to document and define all SOPs to accelerate all activities about manage business process control of IT activities.

Gap Analysis between DISDUKCAPIL's target organization capability level with the capability level that has been achieved at this time can be seen in Table 8 and Figure 3.

Table 8. Gap domain analysis DSS

Sub Domain	Process Name	Current	Expected	Gap
DSS-01	Operations Management	2.1	3	1
DSS-02	Services Requests & Incident Management	2.1	3	1
DSS-03	Problems Management	2	3	1
DSS-04	Continuity Management	2	3	1
DSS-05	Security Services Management	1.1	3	2
DSS-06	Business Process Controls Management	1.1	3	2

5. Conclusions

The conclusion from the results of this research was that some of the existing processes had been implemented well. However, those processes did not reach optimal results expected by the organization.

The average score for both DSS-01 manage operations and DSS-02 Manage Services Requests & Incident were at 2.1, while that of the DSS-03 Manage Problem was 2. The process of DSS-04 Manage Continuity resulted in average value 2. Meanwhile, DSS-05 Manage Security Services, and DSS-06 Manage Business Process Controls, had an average score of 1.1.

There were two processes obtained in level 1 (performed process), namely the DSS-05 and DSS-06. It showed that the processes had been implemented but were not organized and well controlled. Four processes got to level 2 (managed process), namely the DSS-01, DSS-02, DSS-03, and DSS-04

processes. It showed that the processes had been implemented more regularly (planned, monitored, and adjusted) and the resulting work products were determined, well-controlled, and maintained.

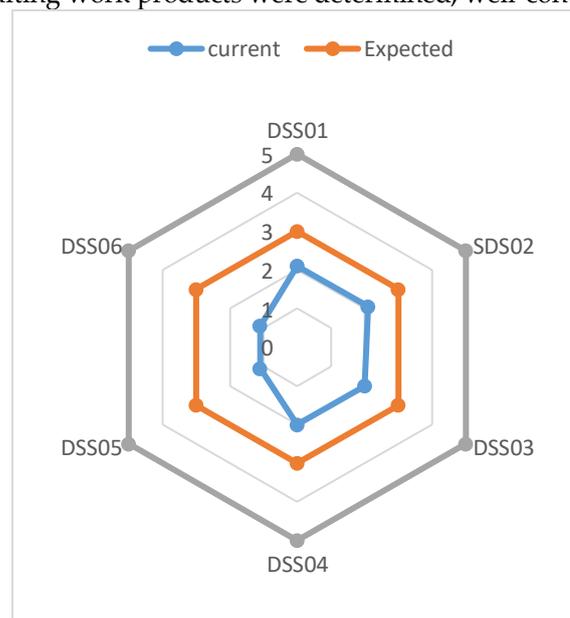


Figure 3. Radar graph of DSS domain capability levels

The researchers hoped that this research and the resulting recommendations can be used by DISDUKCAPIL as a reference to improve the organizational IT Governance.

6. References

- [1] J. F. Andry, "Performance Measurement of Information Technology Governance: A Case Study," *Jurnal Sistem Informasi (Journal of Information System)*, vol. 12, no. 2, pp. 56-62, 2016.
- [2] H. Bin-Abbas and S. H. Bakry, "Assessment of IT governance in organizations: A simple integrated approach," *Computers in Human Behavior*, vol. 32, no. March, pp. 261-267, 2014.
- [3] S. C. B. Barbosa, I. A. Rodello and S. I. D. d. Pádua, "Performance measurement of information technology governance in brazilian financial institutions," *JISTEM - Journal of Information Systems and Technology Management*, vol. 11, no. 2, pp. 397-414, 2014.
- [4] J. F. Andry, "Audit of IT Governance Based on COBIT 5 Assessments: A Case Study," *Jurnal Nasional Teknologi dan Sistem Informasi (TEKNOSI)*, vol. 2, no. 2, pp. 27-34, 2016.
- [5] Y. Ding, "Modelling continued use of information systems from a forward-looking perspective: Antecedents and consequences of hope and anticipated regret," *Information & Management*, vol. 55, no. 4, pp. 461-471, 2018.
- [6] P. Liu, O. Turel and C. Bart, "Board IT Governance in Context: Considering Governance Style and Environmental Dynamism Contingencies," *Information Systems Management*, vol. 36, no. 3, pp. 212-227, 2019.
- [7] I. ISACA, *A Business Framework for the Governance and Management of Enterprise IT*, Rolling Meadows, Illinois, United States: ISACA, 2012.
- [8] P. Zhang, K. Zhao and R. L. Kumar, "Impact of IT Governance and IT Capability on Firm Performance," *Information Systems Management*, vol. 33, no. 4, pp. 357-373, 2016.
- [9] 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)*, vol. 3, no. 1, pp. 21-29, 2013.
- [10] V. Jarsa and K. Christianto, "IT Governance Audit with COBIT 5 Framework on DSS Domain," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 3, no. 4, pp. 279-286, 2018.

- [11] J. F. Andry and A. K. Setiawan, "IT Governance Evaluation Using Cobit 5 Framework on the National Library," *Jurnal Sistem Informasi (Journal of Information System)*, vol. 15, no. 1, pp. 10-17, 2019.
- [12] H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat and C. UtamiPutri, "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk," *Procedia Computer Science*, vol. 124, pp. 569-576, 2017.
- [13] R. Wijaya and J. F. Andry, "Performance measurement of JP soft application using COBIT 5 framework," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no. 2, pp. 83-93, 2017.
- [14] D. Zeglat, W. AlRawabdeh, F. AlMadi and F. Shrafat, "Performance Measurements Systems: Stages of Development Leading to Success," *Interdisciplinary Journal Of Contemporary Research In Business*, vol. 4, no. 7, pp. 440-448, 2012.
- [15] I. W. S. Pramana, P. R. Iswardani and P. A. Mertasana, "IT Governance Evaluation of Hotel Warehouse Section Using the COBIT 5 Framework," *International Journal of Engineering and Emerging Technology*, vol. 3, no. 2, pp. 5-12, 2018.
- [16] T. Huygh and S. D. Haes, "Investigating IT Governance through the Viable System Model," *Information Systems Management*, vol. 36, no. 2, pp. 168-192, 2019.
- [17] I. M. Al-Zwyalif, "IT Governance and its Impact on the Usefulness of Accounting Information Reported in Financial Statements," *International Journal of Business and Social Science*, vol. 4, no. 2, pp. 83-94, 2013.
- [18] A. Mohseni, M. AhmadAliNezhad and S. A. Ghasempoori, "Model of requirements engineering for information technology governance based on the COBIT framework in public organizations using the REGIT method: Case study: Civil registration organization," in *IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, Iran, 2017.
- [19] J. F. Andry and H. Hartono, "Performance Measurement of IT Based on COBIT Assessment: A Case Study," *Jurnal Sistem Informasi Indonesia (JSII)*, vol. 2, no. 1, pp. 1-13, 2017.
- [20] S. Ramlaoui and A. Semma, "Comparative study oComparative of COBIT with other IT Governance Frameworks," *International Journal of Computer Science Issues (IJCSI)*, vol. 11, no. 6, pp. 95-101, 2014.
- [21] S. Ahriz, A. E. Yamami, K. Mansouri and M. Qbadou, "Cobit 5-Based Approach for IT Project Portfolio Management: Application to a Moroccan University," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 4, pp. 88-95, 2018.
- [22] O. Illoh, S. Aghili and S. Butakov, "Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates," in *Service-Oriented Computing - ICSOC 2014 Workshops*, Toumani F. et al (eds) ed., vol. 8954, Cham, Springer, 2015, pp. 236-249.
- [23] M. Wolden, R. Valverde and M. Talla, "The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1846-1852, 2015.
- [24] A. Joshi, L. Bollen, H. Hassink, S. D. Haes and W. V. Grembergen, "Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role," *Information & Management*, vol. 55, no. 3, pp. 368-380, 2018.
- [25] I. ISACA, "COBIT Process Assessment Model (PAM): Using COBIT 5," ISACA, Rolling Meadows, Illinois, United States, 2013.