DOI: 10.14421/ijid.2019.08205 IJID (International Journal on Informatics for Development), *e-ISSN:2549-7448*
Vol. 8, No. 2, 2019, Pp. 74-83

Evaluation of E-Government Using COBIT 5 Framework

(Case Study of Sistem Database Pemasyarakatan Implementation in Ministry of Law and Human Rights in the Special Region of Yogyakarta)

Fanny Novianto[1], Maria Ulfah Siregar[2]
Informatics Department
Faculty of Science and Technology
State Islamic University of Sunan Kalijaga Yogyakarta
[1]fannynovianto@yahoo.co.id, [2]maria.siregar@uin-suka.ac.id

Article History
Received Feb 8th, 2020
Revised Aug 23rd, 2020
Accepted Aug 29th, 2020
Published Dec, 2019

Abstract— **Information technology has become an important element in the industrial era 4.0, an era where the concept of automation is known in the production process carried out by technology by reducing the role of humans in its application. Since the issuance of Presidential Instruction Number 3/2003 concerning National Policies and Strategies for E-Government Development, both central government and local governments, have begun to move to develop e-government in their respective regions. The Ministry of Law and Human Rights of the Republic of Indonesia is currently implementing e-government in internal business processes and public services that aimed at serving prime communities, eliminating illegal payments, and creating transparent and accountable performance. One of them is the use of the Sistem Database Pemasyarakatan (SDP). Data and information in the SDP are confidential because one of them contains data and information on criminals in Indonesia. The research method used is a quantitative method using a questionnaire instrument and using the 5th edition of the COBIT framework model and emphasizes on information security. From the gap analysis, it can be recommended one of them is Organizations must integrate security into every facet of management and operations. This begins with identifying all business processes and associated stakeholders, including audit.**

Keywords—e-government; framework COBIT 5; information security; Capability model

1 INTRODUCTION

Information technology has become an important element in the industrial era 4.0, an era where the concept of automation is known in the production process carried out by technology by reducing the role of humans in its application. The hope of this concept is to reduce the risk of failure, improve the accuracy and efficiency of time at work. This concept can be applied to the industrial, education, health and government sectors. At this time, Information technology in the government or called by electronic government (e-government) is an absolute necessity and must be continuously developed as an acceleration tool in strategic policy and decision making. Utilization of e-government aims to improve performance and productivity, improve budget efficiency, transparency and accountability in the delivery of service activities to the communities.

While the Indonesian government recognizes the benefits of e-government, and has initiated various policies since 2003 to support its implementation (i.e. development of reliable systems and infrastructure, quality and service guidelines and standards, as well as the regulation of public service transactions), these policies have yet to yield substantive results in e-government services in the country [1]. Since the issuance of Presidential Instruction Number 3/2003 concerning about National Policies and Strategies for E-Government Development, both central government and local governments, have begun to move to develop e-government in their respective regions. The application of e-government in government aims to break down long and rigid bureaucratic barriers that hinder interaction between institutions and inhibit partnerships with the business world and open up space for people to participate in developing the nation and state.

Initially the implementation of e-government was slow, starting with the use of websites in government offices as a source of information for the public. The slow development of e-government is because to build information technology facilities and infrastructure requires enormous investments, human resources as managers of information technology experience a transition from traditional serving culture through face to face, long bureaucracy into a culture that is expected to be fast, transparent and accurate and regulation as a legal standing in the implementation of standardized e-government has not been sufficient. At 2011, all central and local governments, including ad-hoc institutions, had websites [2].

The incessant use of e-government in the government both central and regional, of course, not only produces benefit or value to the organization, but also gives a variety of problems and obstacles. To guarantee the benefit and value by using e-government and minimize various problems and obstacles, it is necessary to build information technology governance in the e-government development. In the information technology governance, an organization does not only build information technology facilities and infrastructure, but how information technology is used be able to achieve organizational goals, is able to play a role in the organization's strategic decision making processes and policies and remains in harmony with the architecture framework of information technology development that is has been established.

The Ministry of Law and Human Rights of the Republic of Indonesia is currently implementing e-government in internal business processes and public services. Various innovations have been carried out by the Ministry of Law and Human Rights of the Republic of Indonesia to develop e-government that aimed at serving prime communities, eliminating illegal payments and creating transparent and accountable performance. One of them is the use of the Sistem Database Pemasyarakatan (SDP).

SDP is a comprehensive Information Technology solution that covers all Correctional business processes. SDP is defined as the entire information system which includes the collection, screening, management, presentation and communication of Correctional information. The purpose of developing SDP is to provide correctional information as an effort to improve public services to government agencies, communities and correctional prisoners (WBP), which are effective, efficient, accountable and transparent based on information technology.

To achieve information technology good governance, strategies are needed in developing existing e-government. The first step is to evaluate the implementation of e-government. Evaluation is done by measuring the level of Capability of e-government that has been applied. This measurement includes a strategic plan for information technology management, maintenance of information technology facilities and infrastructure, management of information technology services that are sustainable and the last is oversight of information technology governance.

Data and information in the SDP are confidential because one of them contains data and information on criminals in Indonesia [3]. Only certain data and information with the approval of the Minister of Law and Human Rights of the Republic of Indonesia are permitted to be shared with the public. With the use of information technology and the increasing number of information presented by the government as part of public services, the greater the vulnerability to the security and confidentiality of the information system itself [4].

The scope of this research is e-government which has been implemented in the Ministry of Law and Human Rights in the Special Region of Yogyakarta. The research method used is a quantitative method using a questionnaire instrument and using the 5th edition of the Objective for Information and Related Technology (COBIT) framework model to determine the level of capability in the information technology governance process and emphasizes on information security and provides a detailed and practical description of information security. This study will provide an overview of information technology governance has been implemented and produce recommendations that is needed to improve and develop a comprehensive information technology governance.

However, this research was an extended version of our previous research which determine the maturity level of the information technology governance process [12]. The previous research stated that the current maturity level of the process almost reached the expected maturity level. So, this research was conducted to know the capability in this level of maturity.

2 METHOD

2.1 Study area

2.1.1 E-government

E-government is not a drug or a shortcut to significant improvement or rapid economic growth, or achieving efficiency in government performance in a short time, or establishing clean and transparent governance mechanisms; e-government is a means or tool to get to these objectives [5].

The implementation of e-government is a form of implementing the use of information technology for government services to the public, namely how the government provides information to stakeholders through a web portal. The main reasons for implementing e-government [6] :

1. *E-government improves efficiency;*
2. *E-government improves service quality;*
3. *E-government helps achieve policy outcomes*
4. *E-government contributes to achieving economic objectives*
5. *E-government can be the major contributor to reform*
6. *Builds trust between citizens and government*

2.1.2 COBIT Framework

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector [7].

COBIT 5 is a major strategic improvement providing the next generation of ISACA guidance on the governance and management of enterprise information technology (IT) assets. Building on more than 15 years of practical application, ISACA designed COBIT 5 to meet the needs of stakeholders, and to align with current thinking on enterprise governance and management techniques as they relate to IT.

The COBIT 5 principles and enablers are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

1. *Meeting Stakeholder Needs;*

Governance is about negotiating and deciding amongst different stakeholders' value interests. The governance system should consider all stakeholders when making benefit, resource and risk assessment decisions.

2. *Covering the Enterprise End-to-end;*

Integrates governance of enterprise Information Technology into enterprise governance, the governance system for enterprise Information Technology proposed by COBIT 5 integrates seamlessly in any governance system because COBIT 5 aligns with the latest views on governance. Covers all functions and processes within the enterprise and COBIT 5 does not focus only on the 'Information Technology function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

3. *Applying a Single Integrated Framework;*
4. *COBIT 5 aligns with the latest relevant other standards and frameworks used by enterprises. This allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.*
5. *Enabling a Holistic Approach;*
6. *Separating Governance From Management;*

Governance ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved, setting direction through prioritisation and decision making and monitoring performance and compliance against agreed on direction and objectives (EDM). Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

The five principles enable companies to build effective governance and management frameworks, optimize investment, and use IT to benefit stakeholders [8].

The COBIT 5 process model divides the process of corporate governance and IT management into two process domains, namely:

1. *Governance*, The domain area contains 5 governance processes in the form of Evaluate, Direct, Monitor process domains. Where there is a definition for each process.
2. *Management*, The domain area contains 4 domains, aligned with the area of responsibility of Plan, Build, Run, and Monitor (PBRM), providing end-to-end IT coverage. The domain is the structure of the COBIT 5 domain and process:
   a. Align, Plan, and Organize (APO), Domain that discusses plans, strategies, and focus on achieving business objects. The realization of the vision strategy is needed to be planned, communicated and managed to produce perspective.
   b. Build, Acquire, and Implement (BAI), Providing solutions and services that can be used. To realize the information technology strategy, the technological solutions needed, built or obtained, or already implemented must be in accordance with the business object.
   c. Deliver, Service, and Support (DSS), Domain that discusses the delivery and support of services needed, including operational facilities, user service support and security management.

d. Monitor, Evaluate, and Assess (MEA), Observe all processes to ensure following the directions provided. All information technology processes are needed to be assessed at all times in order to maintain quality and fulfillment of control needs. The domain includes management performance, monitoring internal control, relating to governance.

COBIT 5 Process Capability Model are the assessment task in COBIT 5 is based on ISO/IEC 15504 underlining the strong alignment of this framework with the most generally accepted best practices and standards. The six levels of the COBIT 5 Process Capability Model are :

1. *Level 0 : Incomplete process*

The process is not placed or it cannot reach its objective. At this level the process has no objective to achieve. For this reason this level has no attribute.

2. *Level 1 : Performed process.*

The process is in place and achieves its own purpose. This level has only “Process Performance” as process attribute.

3. *Level 2 : Managed process.*

The process is implemented following a series of activities such as planning, monitoring and adjusting activities. The outcomes are established, controlled and maintained. This level has “Performance Management” and “Work Product Management” as process attributes.

4. *Level 3 : Established process.*

The previous level is now implemented following a defined process that allows the achievement ofthe process outcomes. This level has “Process Definition” and “Process Deployment” as process attributes.

5. *Level 4 : Predictable process.*

This level implements processes within a defined boundary that allows the achievement ofthe processes outcomes. This level has “Process Management” and “Process Control” as process attributes.

6. *Level 5 : Optimising process.*

This level implements processes in the way that makes it possibletoachieve relevant,current and projected business goals. This level has “Process Innovation” and “Process Optimisation” as process attributes.

Table 1. Capability Model Process

Capability Scale	Capability Value	Capability Level
0,00 – 0,50	Level 0	Incomplete Process
0,51 – 1,50	Level 1	Performed Process
1,51 – 2,50	Level 2	Managed Process
2,51 – 3,50	Level 3	Established Process
3,51 – 4,50	Level 4	Predictable Process
4,51 – 5,00	Level 5	Optimizing Process

ISACA defines information security as something that : Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non access when required (availability) [9].

As of COBIT 5, processes such as APO13 Manage Security, DSS04 Manage Continuity and DSS05 Manage Security Services provide basic guidance on identifying, operating and monitoring systems for general security management [10].

The main objective of developing COBIT 5 for Information Security :

1. *Responsibilities for IT functions on information security*
2. *Aspects that will improve the effectiveness of leadership and information security management such as organizational structure, rules and culture*
3. *Information security relationships and networks to enterprise goals*
4. *Maintain security risks at authorized levels and protect information against people who are not authorized or authorized to make modifications that could result in chaos*
5. *Ensuring services and systems can be used sustainably by internal and external stakeholders*
6. *Follow relevant laws and regulations*

Using COBIT 5 for Information Secutiry provides a number of capabilities related to information security for companies so as to generate company benefits such as :

1. *Reduces complexity and increases cost effectiveness due to better and easier integration*
2. *Increase user satisfaction*
3. *Improve the integration of information security within the company.*
4. *Informing risk decisions and risk awareness*
5. *Improve prevention, detection and recovery*
6. *Reducing information security incidents (impacts)*
7. *Increase support for innovation and competitiveness*
8. *Improve the management of costs associated with the information security function.*
9. *Better understanding of information security*

The Principles of Security are as follows [11]:

1. *Confidentiality*: ensuring that certain information can only be accessed by those who are entitled or have the authority to obtain it
2. *Integrity:* protect the accuracy and completeness of information through a number of effective processing methodologies

3. *Availability*: ensuring that the relevant information can be accessed by those in authority as needed

2.2 Procedures

In this study, the stages used are as follows:

1. *Determine the Research Object, this research was conducted on the SDP at the Regional Office of the Ministry of Law and Human Rights in the Special Region of Yogyakarta;*
2. *Observation and literature studies are carried out for information about theories, concepts, methods that are appropriate to the problem;*
3. *Identifying strategic objectives in the development of SDP to determine COBIT 5 enterprise goals;*
4. *From the organizational goals (enterprise goals) that have been set, carried out a mapping of organizational IT goals (IT Related Goals) to determine the processes (domain) in COBIT 5;*

In this research, the selected domains are shown on Table 2

Table 2. Cobit 5 Domain

No	Domain		Practice	
1	Governance	Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance
2			EDM02	Ensure Benefits Delivery
3			EDM03	Ensure Risk Optimisation
4			EDM04	Ensure Resource Optimisation
5			EDM05	Ensure Stakeholder Transparency
6	Management	Align, Plan and Organise	APO01	Manage the IT Management Framework
7			APO04	Manage Innovation
8			APO07	Manage Human Resources
9			APO13	Manage Security
10		Deliver, Service and Support	DSS01	Manage Operations
11			DSS04	Manage Continuity
12			DSS05	Manage Security Services
13		Monitor, Evaluate and Assess	MEA02	Monitor, Evaluate and Assess the System of Internal Control

5. *Making a design of questionnaires that containing statements that are relevant to the process in COBIT 5 emphasize on APO13 and DSS05;*
6. *Identifying respondents related to SDP, in this case the selected respondents are the manager of the SDP, with the following levels:*
   a. Operator: Staff related to the SDP
   b. Supervisor: Head of Sub Division that handles the SDP
   c. Administrator: Head of Sub Division or Staff who handle Information Technology
   d. Super Administrator : Officials at the central level (Directorate General of Corrections) who supervise and coordinate SDP.
7. *Data collection in the form of observations made by directly observing the activities carried out and through the distribution of questionnaires with statements about the level of capability that must be answered by the target. In the questionnaire has an alternative assessment, as follows: Strongly Agree, Agree, Neutral, Disagree and Strongly Disagree;*
8. *Data processing by collecting and compiling in accordance with predetermined domains.*
9. *Data analysis is performed after data processing, consisting of capability analysis, expected capability level and gap analysis;*
10. *Recommendations based on COBIT 5 domain.*

2.3 Data Analysis

Data analysis is carried out by processing each questionnaire statement from respondents regarding the Capability level of the SDP.

This questionnaire contains questions from domain control are shown on Table 3

Table 3. Questions

No	Domain		Statement
1	EDM01	01	The Ministry has plans and procedures related to SDP management
		02	The Ministry has regulations as a legal standing in SDP governance
		03	The performance monitoring process in SDP management continues
		04	The SDP that was developed was in line with the expectations of the stakeholders
2	EDM02	01	The Ministry is able to maintain the quality of SDP services
		02	SDP has an optimal or comparable contribution to IT investments that have been made
3	EDM03	01	The Ministry is able to manage the risks posed by the use of SDP effectively and efficiently
		02	The Ministry is able to handle the risk of damage to SDP facilities and infrastructure
4	EDM04	01	There are priorities in meeting IT resources (SDP) with a limited budget
		02	The Ministry is able to manage IT resources (SDP) optimally
		03	The Ministry is able to find irregularities or problems and report improvements

5	EDM05	01	SDP has a complete, accurate and timely reporting system
		02	The reporting system is in accordance with the needs of stakeholders
		03	There is effective communication between the Ministry and stakeholders
6	APO01	01	The Ministry is able to integrate business process activities manually into SDP
		02	The Ministry is able to manage improvements from the SDP process
7	APO04	01	The Ministry has a plan in the procurement of key IT supporting infrastructure (SDP)
		02	The Ministry applies new innovations in the development of existing SDP
		03	The ministry evaluates the application of the innovations used
8	APO07	01	The Ministry maintains competent human resources in the management of SDP
		02	The Ministry maintains the capabilities and competencies of HR in managing SDP
		03	The Ministry evaluates HR performance in SDP management
9	APO13	01	The Ministry builds and maintains SDP security management
		02	The Ministry define and manage an information security risk treatment plan on SDP
		03	The Ministry monitors and reviews SDP security management
10	DSS01	01	The ministry implements SDP management in accordance with established SOP
		02	The Ministry monitors SDP infrastructure regularly
11	DSS04	01	The Ministry maintains a sustainable SDP development strategy
12	DSS05	01	The Ministry is able to protect SDP against malware
		02	The Ministry is able to manage network and connectivity security
		03	The ministry is manage endpoint security
		04	The ministry is manage user identity and logical access
		05	The ministry is manage physical access to IT assets
		06	The ministry is manage sensitive documents and output devices
		07	The ministry is monitor the infrastructure for security-related events
13	MEA02	01	Internal control systems for IT management are carried out regularly
		02	Monitoring and evaluation of business IT management processes is carried out effectively

93 Respondents participated in filling out questionnaires based on levels in SDP management are shown on Table 4

Table 4. Responden Level

No	Level	Participant
1	Operator	60
2	Supervisor	15
3	Administrator	15
4	Super Administrator	3

Calculation of the level of Capability of each statement in the process at COBIT 5 uses a Likert Scale modification. The analysis includes the current capability analysis, expected capability analysis and gap analysis.

Table 5. Likert Scale

No	Likert Scale	Index
1	Strongly Agree	5
2	Agree	4
3	Neutral	3
4	Disagree	2
5	Strongly Disagree	1

The formula used in the calculation:

$$index = \frac{\sum answer}{\sum question} \quad (1)$$

An expected capability level is obtained from the Strategic Plan document of the Ministry of Law and Human Rights of the Republic of Indonesia 2015-2019 and the value of the capability level is obtained from level 0 to level 5. The target is greater than the current capability level that will be a concern in the preparation of Information Technology.

A gap analysis is process that compares actual performance or results with what was expected or desired. The method provides a way to identify suboptimal or missing strategies, structures, capabilities, processes, practices, technologies or skills, and then recommends steps that will help the company meet its goals.

3 RESULT AND DISCUSSION

3.1 *Expected Capability*

In accordance with the 2015-2019 Ministry of Law and Human Rights Strategic Plan document of the Republic of Indonesia, it is seen that efforts to build integrated, transparent and accountable information technology facilities and infrastructure. The use of the SDP must be sustainable and continuously improved to achieve the organization's vision and mission, so that it can be concluded that the capability level expected to reach Level 5 (Optimized Process) or according to the Capability scale has a value of 4.51 - 5.00.

3.2 *Results of Capability Level Measurement per Domain*

Based on the results of processing the questionnaire data distributed to the manager and person in charge of the SDP, the following assessment results are obtained :

a. Evaluate, Direct and Monitoring (EDM) Domain

Table 6. Evaluate, Direct and Monitoring Result

Domain	Capability Scale	Capability Value	Capability Level
EDM01	4.34	Level 4	Predictable Process
EDM02	4.28	Level 4	Predictable Process
EDM03	4.26	Level 4	Predictable Process
EDM04	4.20	Level 4	Predictable Process
EDM05	4.27	Level 4	Predictable Process

- EDM01, Ensure Governance Framework Setting and Maintenance;

The capability value achieved in the EDM01 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The applicable regulations related to information technology are able to optimize the management of SDP. At this level, the SDP that have been developed have met the expectations of stakeholders, there is careful planning and implementation of good procedures in the management of SDP. To ensure that SDP management runs well, the Ministry of Law and Human Rights of the Special Region of Yogyakarta routinely carries out performance monitoring in the form of Monitoring and Evaluation of SDP implementation in the Work Unit. Not only that, the Directorate General of Corrections as an SDP developer also oversees the performance of SDP implementation in the region and as a supporter if there are obstacles in the application of SDP.

- EDM02, Ensure Benefits Delivery;

The capability value achieved in the EDM02 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

At this level the Ministry of Law and Human Rights is able to maintain the quality of services within the SDP. The use of SDP in public services is able to provide optimal benefits for the community, especially the fulfillment of the human rights of Prisoners. The fulfillment of SDP facilities and infrastructure up to the Work Unit level certainly requires the use of a very large budget, but this Information Technology investment is comparable to the benefits obtained by the Ministry of Law and Human Rights to achieve organizational goals according to its vision and mission.

- EDM03, Ensure Risk Optimisation;

The capability value achieved in the EDM03 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The Ministry of Law and Human Rights is able to manage the risks posed by the use of SDP effectively and efficiently up to the Work Unit level. The facilities and infrastructure of SDP which were damaged can be resolved optimally, so that it does not interfere with performance at the Work Unit.

- EDM04, Ensure Resource Optimisation;

The capability value achieved in the EDM04 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The limited amount of budget in fulfilling Information Technology infrastructure at the Ministry of Law and Human Rights does not make SDP fail in development, because SDP is a top priority in the development of Information Technology infrastructure. The Ministry of Law and Human Rights is also able to optimally manage SDP facilities and infrastructure, this cannot be separated from the continuous performance monitoring of the Work Unit.

- EDM05, Ensure Stakeholder Transparency;

The capability value achieved in the EDM05 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The creation of an effective communication process between the Ministry of Law and Human Rights at the regional and central levels with external stakeholders makes SDP counted nationally. Stakeholders have easy access to data and reports presented in the SDP. The reporting system in the SDP is very transparent and complete in accordance with the needs of each stakeholder.

b. Align, Plan and Organise (APO) Domain

Table 7. Align, Plan and Organize Result

Domain	Capability Scale	Capability Value	Capability Level
APO01	4.14	Level 4	Predictable Process
APO04	4.25	Level 4	Predictable Process
APO07	4.12	Level 4	Predictable Process
APO13	4.19	Level 4	Predictable Process

- APO01, Manage the IT Management Framework;

The capability value achieved in the APO01 sub-domain is located at Level 4 (Predictable Process) where the Ministry of

Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The Ministry of Law and Human Rights is able to integrate the Correctional Activities business processes that were originally in the form of manual activities into the Information Technology process through SDP. In the process of transitioning from a manual into an Information Technology process, of course there are various problems encountered. In this case the Ministry of Law and Human Rights is able to overcome and manage

- APO04, Manage Innovation;

The capability value achieved in the APO04 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The existing SDP which is currently the result of the development of the SDP which began in 2009 has undergone various changes. Innovations continue to be made by the Ministry of Law and Human Rights to develop SDP in accordance with the needs of the Work Unit. In the application of new innovations, the Ministry of Law and Human Rights appoints several regions as pilot projects to test innovations in the SDP and continue to be evaluated until they become services that are ready to be used in other Work Units.

- APO07, Manage Human Resources;

The capability value achieved in the APO07 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The regulation that oversees the SDP specifically regulates the human resources of the manager and person in charge of the SDP. In the regulations governed the duties, authority, sanctions for employees who manage SDP. In addition, the Ministry of Law and Human Rights regularly provides education and training, technical guidance and technical consultation in class directly and through teleconferences to improve the competence of SDP managers. The Ministry of Law and Human Rights is also evaluating the performance of SDP managers. Shifting positions or replacement of SDP managers will be made if there are obstacles in the management of SDP in the Work Unit.

- APO13, Manage Security;

The capability value achieved in the APO13 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

In the case of cyber security, the Ministry of Law and Human Rights has adopted standard cyber security procedures in Indonesia. Periodically the network security testing and evaluation process has been carried out in the SDP. This means that SDP can manage security, plan work plans, monitor and provide reports.

c. Deliver, Service and Support (DSS) Domain

Table 8. Deliver, Service And Support Result

Domain	Capability Scale	Capability Value	Capability Level
DSS01	4.28	Level 4	Predictable Process
DSS04	4.24	Level 4	Predictable Process
DSS05	4.23	Level 4	Predictable Process

- DSS01, Manage Operations;

The capability value achieved in the DSS01 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

In the business process of SDP management, the Ministry of Law and Human Rights ensures that the Standard Operating Procedures that have been set are always used, and there will be a review of procedures that require improvement. Monitoring and Evaluation of SDP facilities and infrastructure is routinely carried out in the Work Unit.

- DSS04, Manage Continuity;

The capability value achieved in the DSS04 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

Innovations in the SDP continue to be developed by the Ministry of Law and Human Rights, not only that, the addition of SDP infrastructure in the Work Unit that is directly related to service to the community continues to be carried out. This is a strategy undertaken by the Ministry of Law and Human Rights to ensure the sustainability of the SDP.

- DSS05, Manage Security Services;

The capability value achieved in the DSS05 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The Ministry of Law and Human Rights is able to manage and protect network and connectivity security. This is because the Ministry of Law and Human Rights has implemented cyber security standards in Indonesia. In addition, the Ministry of Law and Human Rights strictly regulates the access rights of SDP managers, monitors user identities and automatically records the activities of Human Resources using SDP.

d. Monitor, Evaluate and Assess (MEA) Domain

Table 9. Monitor, Evaluate and Assess Result

Domain	Capability Scale	Capability Value	Capability Level
MEA02	4.17	Level 4	Predictable Process

- MEA02, Monitor, Evaluate and Assess the System of Internal Control;

The capability value achieved in the MEA02 sub-domain is located at Level 4 (Predictable Process) where the Ministry of Law and Human Rights at this level has carried out an information technology process in accordance with the established limits to achieve the expected results.

The Ministry of Law and Human Rights has implemented an internal control system on the application of the SDP in the Work Unit. Through Monitoring and Evaluation of SDP as a whole which is carried out by a Team from the central or regional to the Work Unit below it, in addition, an internal audit is conducted on SDP facilities as State Property.

3.3 Gap Analysis

Based on the current capability level analysis as a whole is at level 4 (Predictable Process), when compared to the expected capability level at level 5 (Optimizing Process), there is a gap of 1 level. When viewed from the level of Capability will be explained in the following table:

Tabel 10. Gap Analysis

No	Domain	Capability Scale		
		Current	*Expected (Max)*	*Gap = Expected-Current*
1	EDM01	4,34	5,00	0,66
2	EDM02	4,28	5,00	0,72
3	EDM03	4,26	5,00	0,74
4	EDM04	4,20	5,00	0,80
5	EDM05	4,27	5,00	0,73
6	APO01	4,14	5,00	0,86
7	APO04	4,25	5,00	0,75
8	APO07	4,12	5,00	0,88
9	APO13	4,19	5,00	0,81
10	DSS01	4,28	5,00	0,72
11	DSS04	4,24	5,00	0,76
12	DSS05	4,23	5,00	0,77
13	MEA02	4,17	5,00	0,83

The graphic Capability level of information technology governance in the SDP in the Ministry of Law and Human Rights in the Yogyakarta Special Region is as follows:

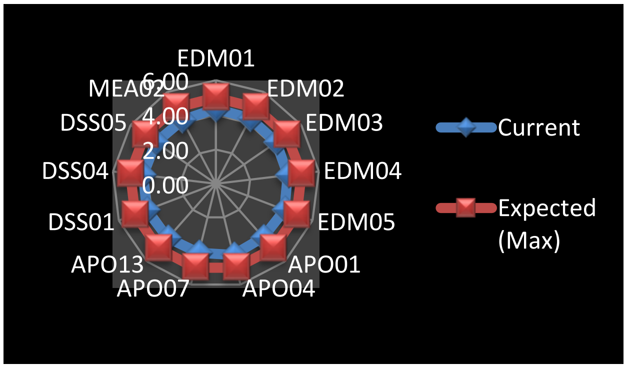

Figure 1. Gap Analysis Graphic based on Capability Level

4 CONCLUSION

From the gap analysis based on the level of Capability, it can be seen that the gap between the current level of Capability and the expected level of Capability is not too large. This means that it is not too difficult for the Ministry of Law and Human Rights of the Special Region of Yogyakarta to continuously develop and improve SDP Information Technology governance to achieve organizational goals and for future needs.

Recommendations given refer to the results of the capability level and gap analysis and can be used as a strategy in developing and optimizing SDP Information Technology governance :

a. Performance monitoring through comprehensive monitoring and evaluation of Information Technology governance in the Work Unit by involving Teams from the regions and Teams from the center as supporters;

b. Involving the community in developing SDP through data and information obtained from the dissemination of community satisfaction surveys;

c. Continue to improve Information security governance in SDP services that is appropriate for the organization;

d. Organizations must integrate security into every facet of management and operations. This begins with identifying all business processes and associated stakeholders, including audit.

REFERENCES

[1] "Challenges in e-government implementation - National - The Jakarta Post." https://www.thejakartapost.com/news/2015/07/27/challenges-e-government-implementation.html (accessed Jan. 12, 2020).

[2] "Sejarah Internet Indonesia:e-government OnnoCenterWiki." https://lms.onnocenter.or.id/wiki/index.php/Sejarah_Internet_Indonesia: e-government (accessed Dec. 21, 2019).

[3] P. M. H. dan H. A. M. R. I. nomor 39 tahun 2016, "Sistem Database Pemasyarakatan," 2016.

[4] A. Wijaya, "Information Security Strategy To Counter Cyber Threats in Electronic Procurement Systems (Study of Hacker Attacks in," vol. 5, pp. 71–86, 2019.

[5] R. E. Indrajit, D. Rudianto, and A. Zainuddin, *Electronic Government in Action*. 2007.

[6] E. Indrayani, *E-Government : Konsep, Implementasi dan Perkembangan di Indonesia*. 2016.

[7] Information Systems Audit and Control Association., *COBIT 5 : a business framework for the governance and management of enterprise IT*. ISACA, 2012.

[8] T. Kristanto, L. Andri Lestari, J. Teknik Informatika, I. Teknologi Adhi Tama Surabaya, and J. Arief Rachman Hakim, "Analisis Tingkat Kematangan E-Government Menggunakan Framework Cobit 5," 2016.

[9] "COBIT 5 Information Security Robert E Stroud CGEIT CRISC," 2012.

[10] "Pengertian dan Fungsi COBIT 5 for Information Security - PROXSISGROUP." https://proxsisgroup.com/pengertian-dan-fungsi-cobit-5-information-security/ (accessed Jan. 10, 2020).

[11] H. Azaim, "Mengenal Confidentiality, Integrity, dan Availability Pada Keamanan Informasi | Netsec Indonesia," Jan. 05, 2017. https://netsec.id/confidentiality-integrity-availability-keamanan-informasi/ (accessed May 03, 2020).

[12] F. Novianto, "Electronic Government Development Strategies Using Frameworks COBIT 5", icse, vol. 3, pp. 263-271, Apr. 2020.