Available online to ejournal.pnc.ac.id

Journal of Innovation Information Technology and Application

Journal Page is available to https://ejournal.pnc.ac.id/index.php/jinita

A Local Government Application Capability Level Information System Audit using COBIT 5 Framework

Bagus Dwi Andika[1], Sucipto[2], Arie Nugroho[3]*

[1-3] Departmen Informatin System, Universitas Nusantara PGRI Kediri, Kediri, Indonesia

email:[1] andika.detelu@gmail.com, [2] sucipto@unpkediri.ac.id, [3] arienugroho@unpkediri.ac.id*

ARTICLE INFO

Article history:
Received 26 June 2023
Revised 20 September 2023
Accepted 21 December 2023
Available online 30 December 2023

Keywords: [Keyword heading]
Information Technology Audit
COBIT 5
Capability level
Gap Analysis

IEEE style in citing this article: B. Dwi Andika, Sucipto, and A. Nugroho, “A Local Government Application Capability Level Information System Audit using COBIT 5 Framework,” A Local Government Application Capability Level Information System Audit using COBIT 5 Framework, vol. 5, no. 2, pp. 130–140, Dec. 2023.

ABSTRACT

The ASN application stores State Civil Apparatus and Employee Work Target master data. ASN application has never been audited. This study aimed to measure the capability level of the ASN application using the COBIT 5 framework. The audit results contain current findings and expectations for the future, then analyze the gaps and make recommendations for improvement. Audit results based on domains DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 achieve capability level 1 performance process. The ASN application manager has successfully implemented a process that has achieved its goals by finding evidence of work product output. To achieve the expected level, namely level 2 managed process, it is recommended that you complete incomplete output documents and carry out activities that have not been carried out per COBIT 5.

1. INTRODUCTION

Sistem Pemerintah Berbasis Elektronik (SPBE) is an Electronic-Based Government System, a government administration that utilizes information and communication technology to provide services to SPBE users[1]–[3]. One of the SPBEs used by the X City Government is the ASN application. This application stores the master data of ASN (State Civil Apparatus) and SKP (Employee Work Target). The benefit of this application is that it holds personnel data and can be used to assess ASN work performance. The government's effort in managing the ASN application is to conduct periodic audits. Information and Communication Technology Audit is a systematic process to obtain and evaluate evidence objectively against information and communication technology assets to determine the level of conformity between information and communication technology with predetermined criteria and standards.

Information technology governance is a branch of corporate governance that focuses on information technology systems and performance and risk management [4]. The definition of an information system audit is evaluating existing evidence used to determine whether a computer system protects assets, data integrity can be maintained, the organization can achieve goals effectively, and efficient use of existing resources[5]. COBIT is developed periodically by ISACA. COBIT is a complete standard and comprehensive scope as an audit framework.[6] then COBIT 5 enables better management of information technology and organization, covering the entire business and functional scope of IT[7].

Corresponding Author : sucipto@unpkediri.ac.id

A RACI diagram is a matrix diagram that shows the parties who play a role in a company or organization. There are four roles on the RACI Chart, namely R (Responsible), A (AccounTable), C (Consulted), and I (Informed). Responsible is the person responsible until the task is completed. Accountable means a person with the right to make a decision. The consulted is a crucial stakeholder who must be involved in all activities. Informed is a person who needs information[8].

The ASN application must be audited to organize good electronic-based regional personnel governance. ASN application governance audits help evaluate organizations so that the level of capability in ASN application governance can be known. The results of the audit evaluation process can be used to improve the implementation of ASN applications maximally. Conduct an audit of ASN applications using the COBIT 5 framework. COBIT management guidelines are issued by ISACA (Information System Audit and Control Association) and ITGI (Information Technology Governance Institute). COBIT is a framework that provides solutions for information technology governance through a domain of processes, activities, objectives, maturity models, and logical and orderly structures [9]. Research discussing information system audits using COBIT 5 was conducted by Gita Natalia Krisnawati in 2019 entitled EVALUATION OF THE APPLICATION OF SIM-RS USING COBIT 5 AT LAWANG HOSPITAL. The differences in the domains discussed are APO 07, BAI 07, and DSS 01 domains.

APO 07 (Manage Human Resources): This process in the APO domain is focused on managing the IT workforce effectively. It involves defining roles and responsibilities, acquiring and developing IT talent, and ensuring that staff is motivated and competent to perform their duties. BAI 07 (Manage IT Human Resources): This process in the BAI domain is closely related to APO 07 but focuses specifically on managing IT human resources during the build and implementation phases. It involves defining IT roles and responsibilities for projects, acquiring and developing IT talent for project teams, and ensuring project staff have the necessary skills and knowledge. DSS01 - Manage Operations: This process involves managing day-to-day IT operations, ensuring that IT services are delivered consistently and by service level agreements (SLAs) and operational standards[10].

The relationship with this study is measuring capability levels, analyzing gaps, and providing recommendations. The results obtained from the study are that the existing capability level is still far from the provisions of the expected capability level, which is level 3. Cobit 5 memiliki 4 level. Level 3: Defined, Level 1: Performed, Level 2: Managed, Level 2: Managed, and Level 4: Predictable[11].

Level 3 is (a) Processes are well-documented and standardized. (b) Roles, responsibilities, and procedures are defined and followed consistently. (c) There is active management and monitoring of processes, including performance measurement. (d) Continuous improvement is a focus, and lessons learned are used for enhancements. Reaching Level 3 maturity in COBIT 5 demonstrates a commitment to process excellence and the ability to deliver reliable and predictable results consistently. It signifies that an organization has well-defined processes that are managed, monitored, and continuously improved to meet business and IT objectives effectively. So, researchers will continue this research to provide recommendations and review improvements for applying SIM-RS Using COBIT 5 at Lawang Hospital, Malang Regency [12].

Research on ASN application governance audits using the COBIT 5 framework has never been conducted. Therefore, it is necessary to conduct research on the ASN application Information System Audit aimed at determining the level of capability of ASN so that it can be used for improvements and recommendations for improving ASN Information System governance.

2. METHOD

Based on Figure 1, the first step is identifying the problem that has never been audited in the ASN application. The author determines the formulation of the problem and conducts a reference study. The author collected data on the analytical tools used in this study are the COBIT 5 standard issued by ISACA using the domains DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 [13]. Some critical processes within the DSS domain in COBIT 5 include DSS01 - Manage Operations: This process involves managing day-to-day IT operations, ensuring that IT services are delivered consistently and per service level agreements (SLAs) and operational standards. DSS02 - Manage Service Requests and Incidents: It handles service requests and incidents from users and stakeholders. This includes incident logging, categorization, prioritization, and resolution. DSS03 - Manage Problems: This process is focused on identifying and addressing the root causes of recurring incidents and problems within the IT environment to prevent them from reoccurring. DSS04 - Manage Continuity: Ensuring business continuity and disaster recovery capabilities are in place to minimize the impact of disruptions on IT services. DSS05 - Manage Security

Services: Managing the security aspects of IT services, including access control, data protection, and security incident management. DSS06 - Manage Business Process Controls: This process ensures that IT services support and align with business processes and that appropriate controls are in place to safeguard data and assets[14].

After the questionnaire is collected, the data will be processed to calculate the level of capability containing current results and future expectations. A gap analysis is carried out to analyze the current status and future expectations. At the final stage, a list of recommendations and improvements is made.

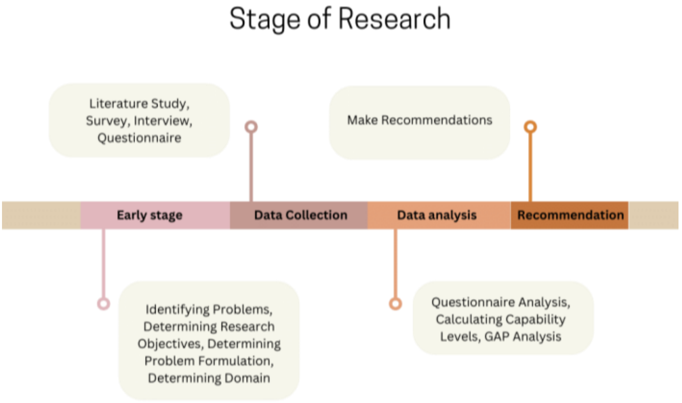
Stage of Research
Literature Study, Survey, Interview, Questionnaire
Make Recommendations
Early stage
Data Collection
Data analysis
Recommendation
Identifying Problems, Determining Research Objectives, Determining Problem Formulation, Determining Domain
Questionnaire Analysis, Calculating Capability Levels, GAP Analysis

Figure 1. Stages of research

This study calculates the process capability levels DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 based on process attributes (PA). Process capability assessments are performed to identify specific groups of process capability. Each attribute defines a particular aspect of the process's capabilities. The combination of achieving these process attributes will determine the level of process capability [15]. Capability level in COBIT 5 as shown in Figure 2 Capability level assessment model.

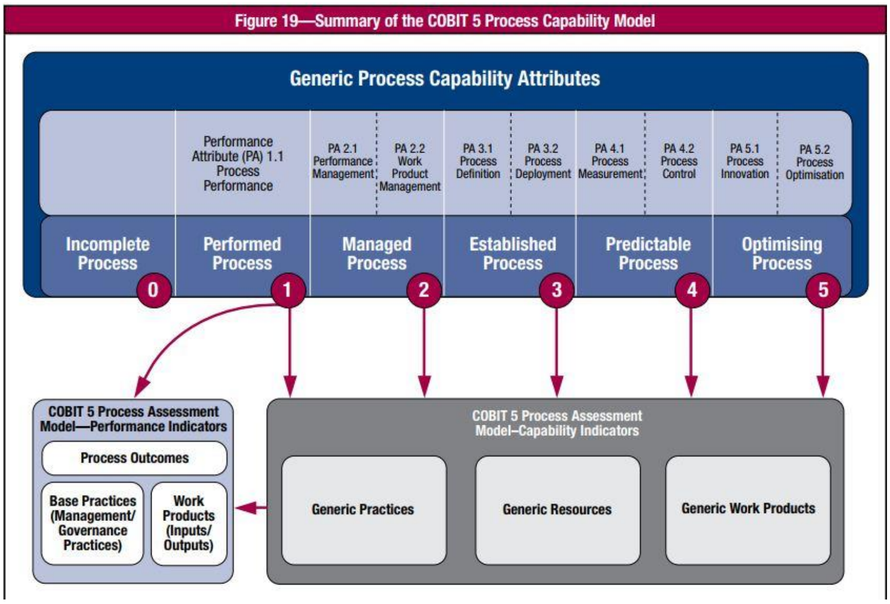
Figure 19—Summary of the COBIT 5 Process Capability Model
Generic Process Capability Attributes
Performance Attribute (PA) 1.1 Process Performance
PA 2.1 Performance Management
PA 2.2 Work Product Management
PA 3.1 Process Definition
PA 3.2 Process Deployment
PA 4.1 Process Measurement
PA 4.2 Process Control
PA 5.1 Process Innovation
PA 5.2 Process Optimisation
Incomplete Process
Performed Process
Managed Process
Established Process
Predictable Process
Optimising Process
0
1
2
3
4
5
COBIT 5 Process Assessment Model—Performance Indicators
Process Outcomes
Base Practices (Management/ Governance Practices)
Work Products (Inputs/ Outputs)
COBIT 5 Process Assessment Model—Capability Indicators
Generic Practices
Generic Resources
Generic Work Products

Figure 2. Process capability assessment model on COBIT 5

The attribute mapping to capability level can be seen in Table 1. The story of process capability used in process assessment consists of six levels, namely [16] :

1. Level 0: *incomplete process*, i.e. the implementation of the process fails to achieve the goal.
2. Level 1: *performed process*, i.e. the implementation of the process can achieve the goal. PA1.1 Process *performance* is a process attribute that reflects level 1 achievement. PA 1.1 measures the extent to which process objectives are achieved. The result of achieving this attribute is reflected in each process producing *the expected* output.

3. Level 2: *managed process*, i.e. the process at level 1 is implemented into a process setting (planned, monitored, and evaluated), and the *work product* of the process is appropriately defined, controlled, and maintained. Its attributes are:
   a. PA 2.1 Performance management: measurement of process implementation arrangements to what extent.
   b. PA2.2 Work product management: Work products are produced by well-regulated processes measured to what extent
4. Level 3: *Established process*; that is, the process at level 2 is implemented using a method that has been defined and can achieve process results. Its attributes are:
   a. PA3.1 *Process definition*: Processes are defined to support the implementation of measured processes to what extent.
   b. PA3.2 *Process deployment*: Process standards implemented effectively are measured to what extent.
5. Level 4: *predicTable process*, the process at level 3 is carried out with defined limits to achieve process results. The attributes are:
   a. PA4.1 *process measurement*: The measurement results are used to ensure that the implementation of the process can support the achievement of organizational goals measured to what extent.
   b. PA4.2 *Process control*: measurement of the extent to which processes are quantitatively arranged to produce a stable and predictable process within defined limits.
6. Level 5: *optimizing process*, i.e. processes at level 4 are improved on an ongoing basis to meet current and future organizational objectives. The attributes contained at this level are:
   a. PA5.1 *Process innovation*: measure the extent to which process change is identified from process implementation and innovation approaches to process implementation.
   b. PA5.2 Process *optimization*: measure the extent to which change is defined and manage process execution effectively to support achieving process improvement objectives.

A rating standard scale based on ISO/IEC 15504 is called *a rating scale* used to measure each process attribute [17]. The scale used to assess process attributes is:

1. N: *not achieved* (0 to 15%).
2. P: *partially achieved* (>15% to 50%)
3. L: *largely achieved* (>50% to 85%)
4. F: *fully achieved* (>85% to 100%)

Table 1. Attribute mapping to capability level

Capability Level	Attribute Process									
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Level 0 - incomplete		NIP								
Level 1 - Performed		L/F								
Level 2 - Managed		F	L/F	L/F						
Level 3 - Established		F	F	F	L/F	L/F				
Level 4 - Predictable		F	F	F	F	F	L/F	L/F		
Level 5 - Optimizing		F	F	F	F	F	F	F	L/F	L/F

Process attributes can be mapped into capability levels, as shown in Table 1. An organization is said to reach a certain level of capability when the details at that level are "fully achieved (F)" or "*largely* achieved (L)", and the attribute values for all levels below *are "fully achieved* (F)". For example, to achieve level 3, the organization must achieve F or L grades for PA3.1, PA3.2, and PA2.1, and PA2.2 must be F. Another example is that although several processes have *been carried out throughout* the base practice and all *work products* have been produced entirely if the organization's overall value does not reach the F scale, there is no need for further level assessments [18].

3. RESULTS AND DISCUSSION

The RACI *Chart* can identify a member's responsibilities and roles in the organization [19]. This study uses the RACI diagram to find suitable and appropriate respondents to fill out the ASN information system audit questionnaire.

Table 2. Research respondents in the RACI Chart

Management Practice	Position	Sum
Head IT Operation	Head of Field	2
Head IT Administrator	Staff IT	25
Total Respond		27

There were 27 respondents consisting of the corresponding parts, as seen in Table 2. Respondents consisted of the Head of Field and IT Staff. Identification of base practices and work products is carried out by the COBIT 5 Process Assessment Model [20], which was then made as material for questionnaires given to 27 respondents who had been identified according to the RACI chart. The self-assessment process is completed by completing questionnaires, observations, and interviews. This self-assessment process will calculate the capability level [21]. After respondents filled out the questionnaire, the capability level measurement process was carried out by recapitulating the DSS01 capability level assessment results, which can be seen in Table 3.

Table 3. Recapitulation of the results of questionnaire processing in the DSS01 process

Recapitulation of Questionnaire Results on *Capability Level Assessment on DSS 01*			
Code	Process Name	%	Achievement
DSS01.01	Performing Operational Procedures	93%	*Fully Achieved*
DSS01.02	Managing IT Service Operations	44%	*Partially Achieved*
DSS01.03	Monitor IT infrastructure	72%	*Largely Achieved*
DSS01.04	Managing Environments	53%	*Largely Achieved*
DSS01.05	Managing Facilities	45%	*Partially Achieved*
	Total	61%	*Largely Achieved*

According to the analysis in Table 3, a recapitulation of the questionnaire results on *the DSS01 capability level* assessment, they concluded that it reached the *Largelly Achieved* (L) scale with a percentage of 61%—recapitulation of questionnaire results on the DSS02 capability level assessment, whose results can be seen in Table 4.

Table 4. Recapitulation of Questionnaire Processing Results in the DSS02 process

Recapitulation of Questionnaire Results on Capability Level Assessment on DSS 02			
Code	Process Name	%	Achievement
DSS02.01	Define Event and service request classification schema	69%	*Largely Achieved*
DSS02.02	Log, classify, and prioritize requests and incidents.	96%	*Fully Achieved*
DSS02.03	Verify, approve, and fulfill service requests	63%	*Largely Achieved*
DSS02.04	Investigate, diagnose, and allocate incidents.	90%	*Fully Achieved*
DSS02.05	Resolving and Recovering from incidents	100%	*Fully Achieved*
DSS02.06	Close service requests and incidents	67%	*Largely Achieved*
DSS02.07	Track status and create reports.	55%	*Largely Achieved*
	Total	77%	*Largely Achieved*

According to the analysis in Table 4, a recapitulation of the results of the DSS02 capability level assessment questionnaire was obtained, and it was concluded that it reached the Largelly Achieved (L) scale with a percentage of 55 percent—recapitulation of questionnaire results on DSS03 capability level assessment whose results can be seen in Table 5.

Table 5. Recapitulation of Questionnaire Processing Results in the DSS03 process

Recapitulation of Questionnaire Results on Capability Level Assessment on DSS 03

Code	Process Name	%	Achievement
DSS 03.01	Identify and classify problems.	71%	*Largely Achieved*
DSS 03.02	Investigate and diagnose problems.	91%	*Fully Achieved*
DSS 03.03	Collect known errors	97%	*Fully Achieved*
DSS 03.04	Resolve and close issues	63%	*Largely Achieved*
DSS 03.05	Proactively manage issues.	58%	*Largely Achieved*
	Total	76%	*Largely Achieved*

According to the analysis in Table 5, a recapitulation of the DSS03 capability level assessment questionnaire results *was* obtained, and it was concluded that it reached the *Largelly Achieved* (L) scale with a percentage of 76%—recapitulation of questionnaire results on DSS04 capability level assessment whose results can be seen in Table 6.

Table 6. Recapitulation of Questionnaire Processing Results in the DSS04 process

Recapitulation of Questionnaire Results on Capability Level Assessment on DSS 04

Code	Process Name	%	Achievement
DSS04.01	Determine business continuity policies, objectives, and scope	72%	*Largely Achieved*
DSS04.02	Maintain a Sustainable Strategy	40%	*Partially Achieved*
DSS04.03	Develop and implement a sustainable business plan	61%	*Largely Achieved*
DSS04.04	Train, test, and review a sustainable business plan (BCP)	33%	*Partially Achieved*
DSS04.05	Review, maintain, and improve sustainability plans	57%	*Largely Achieved*
DSS04.06	Conduct continuity plan training	49%	*Partially Achieved*
DSS04.07	Manage backup settings.	79%	*Largely Achieved*
DSS04.08	Conduct a post-resumption review	36%	*Partially Achieved*
	Total	53%	*Largely Achieved*

According to the analysis in Table 6, a recapitulation of the DSS04 capability level assessment questionnaire results concluded that it reached the *Largelly Achieved* (L) scale with a percentage of 53% results on the DSS05 capability level assessment whose results can be seen in Table 7.

Table 6. Recapitulation of Questionnaire Processing Results in the DSS05 process

Recapitulation of Questionnaire Results on Capability Level Assessment on DSS 05

Code	Process Name	%	Achievement
DSS05.01	Protect against *malware*	87%	*Fully Achieved*
DSS05.02	Manage network and connectivity security	90%	*Fully Achieved*
DSS05.03	Manage endpoint security	92%	*Fully Achieved*
DSS05.04	Manage user identity and logical access	89%	*Fully Achieved*
DSS05.05	Manage physical access to IT assets	82%	*Largely Achieved*
DSS05.06	Manage sensitive devices and outputs	81%	*Largely Achieved*
DSS05.07	Monitor infrastructure for security-related events	73%	*Largely Achieved*
	Total	85%	*Largely Achieved*

According to the analysis in Table 7, a recapitulation of the DSS05 capability level assessment questionnaire results concluded that it reached the *Largelly Achieved* (L) scale with a percentage of 85% recapitulation of questionnaire results on DSS05 capability level assessment, as seen in Table 8.

Table 8. Recapitulation of Questionnaire Processing Results in the DSS06 process

Recapitulation of Questionnaire Results on Capability Level Assessment on DSS06			
Code	Process Name	%	Achievement
DSS06.01	Align control activities embedded in business processes with company goals	43%	*Partially Achieved*
DSS06.02	Control information processing	69%	*Largely Achieved*
DSS06.03	Manage roles, responsibilities, access privileges, and authority levels.	77%	*Largely Achieved*
DSS06.04	Manage errors and exceptions	83%	*Largely Achieved*
DSS06.05	Make sure business information is traceable and accessible	51%	*Largely Achieved*
DSS06.06	Secure accessible information assets	86%	*Fully Achieved*
	Total	68%	*Largely Achieved*

According to the analysis in Table 8, a recapitulation of the DSS06 capability level assessment questionnaire results concluded that it reached the Largelly Achieved (L) scale with a percentage of 68%. Based on the results of filling out questionnaires, interviews, and observations that researchers have carried out, the results of the recapitulation of the achievement of capability level in the ASN application are described in the following six sub-processes:

Table 9. Image of the results of the recapitulation of capability level achievement

NO	Proccess	Level										Target	GAP
		Level 0	Level 1	Level 2		Level 3		Level 4		Level 5			
			PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2		
1	DSS01 Manage Operation		L 69%									2	1
2	DSS02 Manage Service Requests and Incidents		L 77%									2	1
3	DSS03 Manage Problem		L76%									2	1
4	DSS04 Manage Continuity		L 53%									2	1
5	DSS05 Managed Security Services		L 85%									2	1
6	DSS Manage Bussiness Process Control		L 68%									2	1

The capability level assessment starts from level 1; according to the analysis from Table 9, the results of the recapitulation of the achievement of capability levels from the six process domains, namely DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06, show the scale reaching Largely Achieved (L). So, it can be concluded that the ASN application audit process results on the domain are at level 1 and is not continued for the assessment process to level 2 [18]. Level 1 performed process, which means that the process has been implemented and achieved the planned objectives and found evidence of work product output according to the COBIT 5 Process Assessment Model framework [22]. Based on the results of interviews with ASN application managers, the desired level in the DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 sub-processes is at level 2 managed process, namely, the process has been implemented in a more organized way (planned, monitored, and adjusted). The resulting product has been adequately defined, controlled, and maintained [23]. So, it can be concluded that the value of the gap is 1.

After obtaining the capability level achieved at this time and the results of the expected level analysis in the DSS domain and gap analysis, the next step is the formulation of recommendations [24]. Formulation of appropriate recommendations for ASN application managers in the DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 subprocesses.

1. DSS01 subdomain recommendations

   Providing recommendations on DSS01 sub-domains that currently reach level 1 – *performed process to* get level 2 *managed process* include:

   a. Create documents to complete *work product* documents on DSS01 sub-domains, including Internal audit plans, incident tickets, IT facility environmental management reports, IT facility management, and security rules, and create IT asset monitoring rules.

DOI: doi.org/10.35970/ jinita.v5i2.1971

b. Plan internal audits at least one time in 2 years.
c. Monitor event logging so incident tickets are created promptly.
d. Plan environmental and IT infrastructure management rules
e. Plan staff capacity building in the management of IT infrastructure and environment.

2. DSS02 subdomain recommendations

Providing recommendations on DSS02 sub-domains that currently reach level 1 – performed process to get level 2 *managed process* include:

a. Improve the complaint reporting system by adding features of complaint criteria, approved service requests, service requests that have been completed, and service satisfaction ratings from users of the disruption reporting system for services provided by officers. With this feature and making a resume, it will be able to fulfill *work product documents* on the DSS02 sub-domain.
b. Monitor incident reports to be generated promptly
c. Evaluation of service requests and nuisance complaint procedures.
d. Analyze trends in service requests and incidents that occur

3. DSS03 subdomain recommendations

Providing recommendations on DSS03 sub-domains that currently reach level 1 – *performed process to* get level 2 *managed process* include:

a. Create documents to complete *work product* documents in DSS03 sub-domains, including Problem classification scheme documents, documents on the results of studying problems that occur, Problem monitoring reports, and ongoing problem solution documents.
b. Create a problem management catalog that is used to register and report identified issues and to establish an audit trail of the problem management process, which includes the status of each case (i.e., unworked on, in progress, or completed).
c. Monitor the issue resolution process to get regular reports on the progress of troubleshooting during the troubleshooting process.
d. Conduct regular meetings to discuss problems/incidents that have been identified and plan corrective steps.
e. Monitor changes resulting from problem-solving process activities (e.g. problem fixes and identified errors) and report them to superiors to estimate possible costs if improvements occur.
f. Identify problems and document permanent repair solutions to address the root cause systematically

4. DSS04 subdomain recommendation

Providing recommendations on DSS04 sub-domains that currently reach level 1 – *performed process to* get level 2 *managed process* include:

a. Create documents to complete *work product* documents on DSS04 sub-domains, including Current business continuity capability and gap assessment documents, business impact analysis documents, continuity requirements, Approved strategic recommendation documents, Documents containing actions to deal with incidents, sustainable business plan documents, test objectives documents, practice test documents, test result documents and recommendations for testing business plans Continuous, continuity plan review documents, plan change recommendation documents, training requirements documents, post-restart reports after incidents, plan change approval documents.
b. Identify business processes and service activities critical to the ASN application's continuity.
c. Plan, monitor, and evaluate ASN application continuity strategies in response to disruptions to obtain time and cost-saving options.
d. Develop and implement plans to effectively maintain business continuity in responding to incidents in the event of disruption
e. Plan and conduct regular continuity testing to implement the recovery plan against predetermined outcomes and develop recommendations to improve the continuity plan.
f. Conduct periodic continuity capability reviews to ensure continued suitability, adequacy, and effectiveness. Manage plan changes through the change control process to maintain continuity plans.
g. Plan training on procedures, roles, and responsibilities of staff in case of disruption.
h. Determine backup data retention requirements with accessibility in mind.

i. Assess the capability of a sustainable business plan after resuming business processes and services following a disruption/incident.

5. DSS05 subdomain recommendations

Providing recommendations on DSS05 sub-domains that currently reach level 1 – *performed process to* get level 2 *managed process* include:

a. Create documents to complete *work product documents* on DSS05 sub-domains, including Incident ticket documents.
b. Ensure and monitor access to IT assets (server rooms, buildings, areas, or zones) based on job functions and responsibilities. Also, perform monitoring of all entry points to the IT site. Register all visitors who enter IT assets. Furthermore, limit access to sensitive IT assets by setting perimeter boundaries, such as fences, walls, and security devices on interior and exterior doors. Ensure the device records the entry and triggers an alarm in case of unauthorized access. In the process of improving security, it is necessary to carry out regular physical security awareness training.
c. It is necessary to establish procedures for regulating the receipt, use, transfer, and disposal of unique forms. In establishing procedures, it is essential to inventory sensitive documents and output devices and perform regular reconciliation. It is also necessary to physically protect particular structures and sensitive devices appropriately.
d. It is necessary to maintain evidence collection procedures that align with forensic evidence rules and socialize all staff so that all staff know the requirements.
e. Ensure security incident tickets are created promptly when monitoring identifies potential security incidents.

6. DSS06 subdomain recommendations

Providing recommendations on DSS06 sub-domains that currently reach level 1 – performed process to get level 2 managed process include:

a. Create documents to complete *work product documents on* DSS06 sub-domains, including complete records on the results of processing effectiveness reviews, analysis documents and recommendations for the leading causes, information processing control report documents, retention requirements documents,
b. Improve the identification and documentation of crucial business process control activities to meet the requirements of strategic, operational, reporting, and compliance control objectives. In addition, continuously improving the design and operation of ASN process control is necessary.
c. Perform business process activities and control ASN applications by correcting and resending incorrect data without compromising the initial transaction authorization level.
d. Improve data integrity and validity during the processing cycle. Verify the accuracy and completeness of the output.
e. Periodically review the allocation of access rights and privileges based on predefined job roles. Also, allocate roles for sensitive activities so that there is a clear separation of duties.
f. Establish and maintain procedures for assigning ownership, correcting errors, ruling out mistakes, and handling unbalanced conditions.
g. Establish retention requirements based on business requirements to meet operational, financial reporting, and compliance needs. Dispose of source information, supporting evidence, and transaction records by retention policies.
h. Implement data classification, acceptable use, and security policies and procedures to protect information assets. And identify and implement processes, tools, and techniques to properly verify compliance.

4. CONCLUSION

Based on the ASN information system audit analysis results, the DSS01, DSS02, DSS03, DSS04, DSS05, and DSS06 domains achieved capability level 1 perform process in ASN application management. It can be concluded that the ASN application manager has completed the goal by finding evidence of work product output according to the COBIT 5 Process Assessment Model framework. Suggestions for future research can use domains other than DSS to determine the development of the level of capability in other related fields or subdomain process chains, including EDM (Evaluate, Direct, and Monitor), MEA (Monitor, Evaluate and Assess), APO (Align, Plan and Organize) and BAI (Build, Acquire and Implement).

And for further research, you can conduct audits using other frameworks such as ITIL (Information Technology Infrastructure Library) and COBIT 2019.

REFERENCES

[1] N. S. Warman, S. Syamsir, M. Maldini, O. Nurhasanah, N. R. Oktariandani, and I. H. Syafikruzi, “Implementasi Inovasi Kebijakan Dalam Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Kota Pekanbaru,” *Prosiding Seminar Nasional Pendidikan, Bahasa, Sastra, Seni, dan Budaya*, vol. 1, no. 2, pp. 132–148, Nov. 2022, doi: 10.55606/MATEANDRAU.V1I2.161.

[2] R. Bisma, “Manajemen Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan,” *JIEET (Journal of Information Engineering and Educational Technology)*, vol. 6, no. 2, pp. 73–79, Dec. 2022, doi: 10.26740/JIEET.V6N2.P73-79.

[3] I. M. Sukarsa *et al.*, “Evaluation of E-Government Maturity Models in Sub-District Public Services in Indonesia Using the SPBE Framework,” *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 2, pp. 243–253, Apr. 2020, doi: 10.29207/RESTI.V4I2.1825.

[4] W. Riyadi, “Analisis Sistem Informasi Akademik dengan Cobit framework,” *Jurnal Ilmiah Media Sisfo*, vol. 12, no. 1, pp. 954–965, 2018.

[5] M. Muzaemi, “Audit Sistem Informasi dan Peran Auditor,” *Jurnal Riset Akuntansi dan Bisnis*, vol. 2, no. 2, pp. 22–47, 2016.

[6] M. I. Wiradipta, “Audit Teknologi Informasi dengan menggunakan Framework Cobit 5 Domain Dss (Deliver, Service, And Support) pada Rumah Sakit Umum Dr. Etty Asharto Batu Skripsi Oleh: Muhammad Iqbal Wiradipta Nim. 11650105 Jurusan Teknik Informatika Fakultas Sains Dan Teknol,” p. 117, 2018.

[7] M. W. Astuti, Suprapto, and A. R. Perdanakusuma, “Evaluasi Teknologi Informasi menggunakan COBIT 5 Fokus Proses DSS02 , DSS03 , dan DSS04 (Studi Kasus : PT . Garam (Persero)),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 9, pp. 8874–8881, 2019.

[8] A. Nurlinda Thamrin, “Framework Cobit 5 untuk Audit Tata Kelola Teknologi Informasi (Studi Kasus: Diskominfo Kota Palopo) Cobit 5 Framework for Information Technology Governance Audit (Case Study: Diskominfo Palopo City),” *Jurnal_Pekommas_Vol._6_No*, vol. 2, pp. 9–15, 2021, doi: 10.30818/jpkm.2021.

[9] P. H. Sinta, I. P. A. Swastika, and I. G. L. A. Raditya Putra, “Evaluasi Tata Kelola Teknologi Informasi berbasis COBIT 5 pada Badan Pendapatan Daerah Kabupaten Badung,” *Jurnal Teknologi dan Ilmu Komputer Prima (JUTIKOMP)*, vol. 2, no. 2, p. 1, 2019, doi: 10.34012/jutikomp.v3i1.647.

[10] A. C. Amorim, M. Mira da Silva, R. Pereira, and M. Gonçalves, “Using agile methodologies for adopting COBIT,” *Inf Syst*, vol. 101, p. 101496, Nov. 2021, doi: 10.1016/J.IS.2020.101496.

[11] A. Joshi, J. Benitez, T. Huygh, L. Ruiz, and S. De Haes, “Impact of IT governance process capability on business performance: Theory and empirical evidence,” *Decis Support Syst*, vol. 153, p. 113668, Feb. 2022, doi: 10.1016/J.DSS.2021.113668.

[12] R. F. Gita Natalia Krisnawati, Sucipto, “Evaluasi Penerangan SIM-RS Menggunakan Cobit 5 pada RSUD Lawang,” *Jurnal Ilmiah Teknik Informatika*, vol. 13, no. 2, pp. 80–89, 2019, doi: 10.35457/antivirus.v13i2.858.

[13] ISACA, *Enabling Processes, skills, and knowledge through the globally respected Certified Information Systems Auditor ® (CISA ®)*. 2012.

[14] F. Maciá Pérez, J. V. Berna Martinez, and I. Lorenzo Fonseca, “Strategic IT alignment Projects. Towards Good Governance,” *Comput Stand Interfaces*, vol. 76, p. 103514, Jun. 2021, doi: 10.1016/J.CSI.2021.103514.

[15] A. D. Farida, “Pengukuran Tingkat Kapabilitas Manajemen Risiko Sistem Informasi Koperasi Syariah Menggunakan Framework Cobit 5,” *Jurnal Komputasi*, vol. 8, no. 1, pp. 1–14, 2020, doi : 10.23960%2Fkomputasi.v8i1.2528

[16] R. E. Putri, “Penilaian Kapabilitas Proses Tata Kelola TI Berdasarkan Proses DSS01 Pada Framework COBIT 5,” *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi*, vol. 2, no. 1, pp. 41–54, 2016, doi:10.24014/coreit.v2i1.2181 .

[17] A. R. Audi Kresna Fathurino, Yusi Tyroni Mursityo, “Evaluasi Tata Kelola Sumber Daya Teknologi Informasi Evaluation of Information Technology Resources Governance Using the Cobit 5 Framework Subdomain Edm04 , Apo07 and Dss03 At Port Service Company Pt . Xyz,” vol. 9, no. 5, pp. 1011–1018, 2022, doi: 10.25126/jtiik.202294625.

[18] A. Revansyah, A. Wedhasmara, P. E. Sevtiyuni, and A. Putra, “Pengukuran Tingkat Kapabilitas Teknologi Informasi Pada Sistem Adovelin Warehouse Inventory Sistem (Awis) Menggunakna Cobit 5” Universitas Bina Insan Lubuklinggau JUSIM (Jurnal Sistem Informasi Musirawas) Uni,” vol. 7, no. 2, pp. 114–126, 2022, doi:10.32767/jusim.v7i2.1535 .

[19] D. Putra Muliawan and A. Rachmadi, “Evaluasi Tata Kelola Teknologi Informasi dan Manajemen Sumber Daya Berdasarkan Cobit 5 Domain DSS01, DSS05, dan EDM04 (Studi Kasus: PT. PLN UIP JBTB II),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Vol. 5, No. 4, pp. 1561-15668 April 2021.

[20] ISACA, *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5*. 2013.

[21] D. I. Agselmora *et al.*, “Audit Teknologi Informasi Menggunakan COBIT 5 Domain DSS Pada Universitas Stikubank Semarang,” vol. 9, no. 4, pp. 2804-2814, 2022, doi: 10.35957/jatisi.v9i4.2612.

[22] A. P. Rabhani *et al.*, “Audit Sistem Informasi Absensi pada Kejaksaan Negeri Kota Bandung Menggunakan Framework Cobit 5,” *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 2, pp. 275–280, Aug. 2020, doi: 10.32736/sisfokom.v9i2.890.

[23] E. Yuni, P. M. Akuntansi, F. Ekonomika, and D. Bisnis, “Evaluasi Perencanaan Manajemen Teknologi Informasi Dengan Pendekatan Cobit 5 Framework (Studi pada Dinas Komunikasi dan Informatika Kabupaten Pringsewu),” Vol 6, No 3, 2018, doi: 10.22146/abis.v6i3.59072.

[24] Y. I. Putri and A. D. Herlambang, “Penilaian Kapabilitas Penerapan Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi pada PDAM Kota Malang Jawa Timur),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 11, pp. 4855–4862, 2018.