Capability Analysis in IT Governance for Enhancing SIMPEG Services Using the DSS Domain of COBIT 2019

Andreas Ghanneson Nainggolan, Rian Farta Wijaya

Abstract

The increasing reliance on information technology in public sector organizations requires effective IT governance to ensure service quality and operational efficiency. The Personnel Management Information System (SIMPEG) plays an important role in supporting administrative services; however, issues such as lack of standardization and limited monitoring indicate the need for evaluation. This study aims to analyze the capability level of IT governance in enhancing SIMPEG services using the Deliver, Service, and Support (DSS) domain of the COBIT 2019 framework. The DSS domain focuses on operational service delivery, including operations management, incident handling, problem management, service continuity, security services, and business process controls. This research adopts a mixed-method approach, combining interviews, observations, questionnaires, and document analysis. The capability level is measured using the Process Assessment Model (PAM) to evaluate the current condition (as-is) and the expected target (to-be), followed by a gap analysis to identify areas for improvement. The results show that the overall capability level is at Level 2 (Managed Process). Detailed findings indicate DSS01 = Level 3, DSS02 = Level 2, DSS03 = Level 3, DSS04 = Level 3, DSS05 = Level 3, and DSS06 = Level 3, with a target of Level 3 (Established Process). The gaps are mainly related to the absence of standardized procedures, limited documentation, and insufficient monitoring. The gap analysis reveals several key issues, including the absence of formal Standard Operating Procedures (SOPs), limited documentation practices, inconsistent incident and problem management, insufficient continuity planning, and incomplete implementation of security and control mechanisms. In conclusion, the application of the COBIT 2019 DSS domain provides a structured and effective approach to evaluating and improving SIMPEG services. Achieving Level 3 capability will enhance process standardization, improve service quality, and strengthen the alignment between IT governance and organizational objectives.

Keywords: *IT Governance, COBIT 2019, DSS Domain, Capability Level, SIMPEG*

Andreas Ghanneson Nainggolan[1]
[1]Information Technology, Universitas Pembangunan Panca Budi, Indonesia
e-mail: andreas.nainggolan89@gmail.com[1]

Rian Farta Wijaya[2]
[2]Information Technology, Universitas Pembangunan Panca Budi, Indonesia
e-mail: rianfartawijaya@dosen.pancabudi.ac.id[2]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The rapid advancement of Information Technology (IT) has significantly transformed organizational operations, particularly in government institutions where IT plays a crucial role in improving efficiency, effectiveness, and service quality. In this context, IT governance has become an essential component to ensure that IT resources are aligned with organizational objectives and deliver optimal value. Effective IT governance enables organizations to manage risks, optimize resources, and support decision-making processes in achieving strategic goals [5].

One of the critical implementations of IT in the public sector is the Personnel Management Information System (SIMPEG), which is used to manage employee data and support administrative processes. SIMPEG serves as an integrated system that facilitates the storage, processing, and utilization of personnel data to enhance administrative services and decision-making within government agencies [8]. However, despite its importance, many organizations still face challenges in ensuring that SIMPEG operates effectively and aligns with governance standards, including issues related to system performance, service reliability, and operational procedures.

To address these challenges, the implementation of a structured IT governance framework is necessary. The COBIT 2019 framework, developed by ISACA, provides comprehensive guidelines for managing and governing enterprise IT. It emphasizes aligning IT processes with business objectives, optimizing risk management, and ensuring the effective delivery of IT services [7].COBIT 2019 also introduces a flexible and scalable approach that allows organizations to evaluate and improve their IT governance practices based on capability levels.

Within COBIT 2019, the Deliver, Service, and Support (DSS) domain plays a vital role in ensuring that IT services are delivered efficiently and effectively. This domain focuses on operational processes, including service delivery, problem management, and system support, which are essential for maintaining the performance and reliability of IT systems [3]. Evaluating the capability level within the DSS domain allows organizations to identify gaps between current performance (as-is) and expected targets (to-be), thereby providing a foundation for continuous improvement.

Previous empirical studies have demonstrated the efficacy of utilizing COBIT frameworks across various service environments. For instance, Nugroho [7] conducted a comprehensive evaluation using the COBIT 2019 DSS domain at PT Garam, demonstrating how targeted capability assessments can map critical functional gaps and yield strategic standard operating procedure (SOP) recommendations to elevate enterprise service maturity. Similarly, Syahputra [10] deployed the COBIT 2019 model to audit the E-Kinerja employee performance appraisal platform at a regional Kominfo department, calculating precise mathematical capability gaps between current performance (as-is) and ideal organizational targets (to-be). In the education sector, Manalu [5] utilized the COBIT model to pinpoint how deficiencies in formal policy documentation, coupled with human resource gaps, could actively limit the efficacy of an institution's primary software infrastructure, emphasizing the urgent need for structured optimization frameworks.

Based on these considerations, this study aims to analyze the capability level of IT governance in enhancing SIMPEG services using the DSS domain of COBIT 2019. By conducting a capability assessment and gap analysis, this research is expected to provide insights and recommendations that can improve the effectiveness of SIMPEG services and support better IT governance practices in government institutions.

Literature Review

A. IT Governance and COBIT 2019 Framework

Information Technology (IT) governance functions as an integral part of enterprise governance, providing the structural oversight required to ensure that an organization’s IT infrastructure directly sustains and extends its strategic objectives [5]. As public sector and

state-owned institutions expand their dependency on digital frameworks, systematic evaluation mechanisms become critical to prevent financial inefficiencies and operational operational friction [2]. Within this context, the Control Objectives for Information and Related Technology (COBIT) 2019 framework, developed by ISACA, represents a major evolutionary leap from older governance standards. While preceding frameworks like COBIT 5 utilized a static model across generic domains, COBIT 2019 introduces customizable "design factors" that allow organizations to dynamically tailor their IT governance solutions based on specific risk profiles, technological environments, and institutional mandates [9].

The COBIT 2019 framework splits governance and management activities into five core domains across two central areas. Governance objectives are housed within the Evaluate, Direct, and Monitor (EDM) domain. Meanwhile, Management objectives are partitioned into four operational domains: Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA) [12]. To evaluate performance metrics, COBIT 2019 deploys a continuous Capability Level scale inherited from the ISO/IEC 15504 standard, ranging from Level 0 (complete lack of capability) to Level 5 (continuous optimization), providing a quantitative baseline to measure process execution and formalized work products [1].

B. The Deliver, Service, and Support (DSS) Operational Domain

The management of operational technology execution within the COBIT 2019 architecture is heavily anchored within the Deliver, Service, and Support (DSS) domain. While strategic domains focus on planning and structural implementation, the DSS domain prioritizes the operational back-end, including day-to-day service delivery, data asset protection, and operational continuity [7].The DSS domain is segmented into six operational sub-processes:

1. DSS01 (Managed Operations): Focuses on the execution of routine IT operational procedures and administrative workflows.
2. DSS02 (Managed Service Requests and Incidents): Coordinates the rapid resolution of user requests and technical incidents to sustain operational continuity.
3. DSS03 (Managed Problems): Dedicated to identifying and resolving the root causes of recurring technical issues to eliminate systemic vulnerabilities.
4. DSS04 (Managed Continuity): Establishes disaster recovery protocols and business resilience parameters to avoid prolonged service outages.
5. DSS05 (Managed Security Services): Protects localized information assets and core networks from unauthorized access and cyber threats.
6. DSS06 (Managed Business Process Controls): Assures information processing integrity within functional application frameworks to secure corporate records.

For specialized human resource applications like the *Sistem Informasi Manajemen Kepegawaian* (SIMPEG), auditing the DSS domain is essential to confirm that personnel records are securely maintained, user incidents are systematically tracked, and daily workflows run without structural disruption.

C. Capability Level and Gap Analysis

Capability level assessment is a key component of IT governance evaluation using COBIT frameworks. It measures the extent to which IT processes are implemented and managed effectively. The assessment is typically conducted using the Process Assessment Model (PAM), which evaluates process performance based on defined attributes and indicators [8].

Gap analysis is used to compare the current capability level (as-is) with the desired level (to-be). This analysis helps organizations identify deficiencies and determine necessary improvements to achieve higher capability levels. Previous studies have shown that many organizations are still at lower capability levels, indicating the need for structured

improvements such as developing standard operating procedures (SOPs), improving documentation, and enhancing process management [5].

D. Empirical Evaluations on Personnel and Public Sector Information Systems

The evaluation of human resource and public sector platforms via standardized frameworks has been explored across multiple methodologies. Harjo [3], utilized COBIT 2019 design factors within a public personnel institution (Instansi Kepegawaian XYZ) to pinpoint critical operational gaps, identifying that the DSS02 (Managed Service Requests and Incidents) sub-domain required immediate remediation to optimize staff placement and professional development tracking. Furthermore, empirical assessments using COBIT configurations have illuminated recurring operational challenges in administrative architectures. Permatasari [8], audited the SIMPEG platform at the Government Office of Kediri City using the DSS01 and DSS03 domains of COBIT 5, showing that while basic functional operations were executed by technical staff, the lack of formalized standard operating procedures (SOPs) restricted the system's long-term efficiency. This documentation bottleneck is consistently reflected across broader public frameworks, Syahputra [10], used COBIT 2019 to evaluate an E-Kinerja employee performance appraisal system at a regional Communication and Information (Kominfo) office, utilizing precise capability gap calculations to demonstrate that misalignments between actual capabilities (*as-is*) and organizational targets (*to-be*) frequently stem from a lack of formal oversight and non-standardized workflows.

Similarly, Manalu [5], noted that during a multi-domain IT audit of institutional software systems, even when base practices are adequately performed, the systematic absence of verified documentation or "Work Products" severely suppresses capability level advancement. In corporate environments, such as the ERP evaluations performed by Nugroho [7] at PT Garam or the SaaS platform audits conducted by Firmansyah [1] at PT Solusi Finansialku Indonesia, the deployment of the COBIT 2019 DSS domain has proven that creating prescriptive, documentable recommendations is the most effective approach to elevate an enterprise's operational capacity and ensure overall service reliability.

E. Literature Synthesis and Research Gap

A synthesis of the existing literature indicates that while the COBIT framework has been widely applied to assess diverse digital systems ranging from state-owned ERP systems [7] to corporate SaaS models [1] and regional performance tracking systems [10] there remains an empirical gap in the holistic evaluation of human resource systems like SIMPEG using the updated COBIT 2019 framework. Previous SIMPEG evaluations either relied on older models such as COBIT 5 [8], which lack modern adaptive design factors, or utilized alternative alignment models like Luftman's SAMM [2], which prioritize strategic alignment over technical process execution.

Additionally, research focusing on personnel agencies often isolates only a single sub-domain, such as DSS02 [3]. Given the widespread lack of structured operational documentation identified in public institutions [5], a comprehensive evaluation across the entire DSS domain (DSS01–DSS06) using COBIT 2019 is necessary. This study addresses this gap by analyzing all six sub-domains of the COBIT 2019 DSS domain within a SIMPEG service environment, establishing a clear path to bridge operational gaps, secure personnel data integrity, and enhance public sector service delivery.

Research Methodology

This study adopts a structured operational audit and quantitative descriptive approach to assess and enhance the Information Technology (IT) governance capability of the *Sistem Informasi Manajemen Kepegawaian* (SIMPEG) services. The methodology is systematically mapped into four sequential phases: (1) Research Initiation and Domain Mapping, (2) Data Collection and Operational Sampling, (3) Capability Level and Gap Analysis, and (4)

Prescriptive Improvement Mapping. The overarching research framework is illustrated in Figure 1.

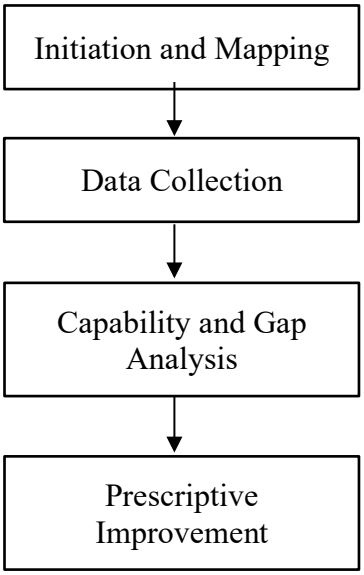

Figure 1. Research Methodology

A. Research Initiation and Domain Mapping

The initial phase begins with a comprehensive institutional assessment to understand the core strategic goals and operational boundaries of the SIMPEG environment [2]. To ensure that the audit aligns with the institution's specific organizational attributes, the study utilizes the formal COBIT 2019 Design Factors toolkit [4]. These design factors including enterprise strategy, goals, risk profile, and infrastructure landscape are calculated using the standardized COBIT 2019 Excel-based design tool to pinpoint the most critical processes [9].

While the high-level assessment establishes tailored organizational priorities, this study strictly focuses on the operational execution tier by isolating the entire Deliver, Service, and Support (DSS) domain. This targeted scope ensures a granular evaluation of all six sub-domains: Managed Operations (DSS01), Managed Service Requests and Incidents (DSS02), Managed Problems (DSS03), Managed Continuity (DSS04), Managed Security Services (DSS05), and Managed Business Process Controls (DSS06) [12].

B. Data Collection and Operational Sampling

To secure high-validity primary and secondary data, a multi-method data collection approach is deployed [10]. Primary data is gathered through structured interviews and customized questionnaires distributed to key stakeholders involved in the SIMPEG ecosystem, including IT managers, human resource administrators, and technical support personnel [1]. The questionnaire parameters are derived directly from the COBIT 2019 Governance and Management Objectives guide, translating specific "Base Practices" into measurable operational indicators [11].

Simultaneously, secondary data collection focuses on a rigorous document review to verify the existence of organizational "Work Products," such as standard operating procedures (SOPs), incident logs, disaster recovery plans, and logical security matrices. As emphasized by [8], verifying formal documentation is mandatory; the physical absence of verified work products prevents an organization from advancing to higher capability tiers, even if technical workflows are actively performed by staff.

Table 1. Respondents

Management Practice	Department	Total

Chief Information Office	Head of Procurement, Dismissal and Information Division	1
Head IT Operation	Head of Data and Information	1
Service Management	Staf of Data and Information	10
	Total	12

C. Capability Level and Gap Analysis

The computation of capability levels is conducted in strict accordance with the COBIT 2019 performance management architecture, which scales from Level 0 to Level 5 based on the ISO/IEC 15504 process assessment model [1]. For each sub-domain (DSS01 to DSS06), the compliance rate of individual activities and work products is mathematically calculated. The compliance rating is classified based on the standard COBIT framework:

- **N (Not Achieved):** 0% to 15% achievement of the process attributes.
- **P (Partially Achieved):** >15% to 50% achievement.
- **L (Largely Achieved):** >50% to 85% achievement.
- **F (Fully Achieved):** >85% to 100% achievement.

A specific capability level (Level 2 or Level 3) is considered fully achieved only if all underlying activities and mandatory work products pass the "Fully Achieved" (>85%) threshold. Once the current capability score (As-Is) is established, it is compared against the institution's targeted maturity level (To-Be), which represents the ideal governance tier required to support the administrative scope of SIMPEG. The difference between these two parameters defines the operational capability gap (GAP), expressed as:

GAP = Target Capability Level (To-Be) - Current Capability Level (As-Is)

This gap calculation explicitly highlights the critical bottlenecks, technical vulnerabilities, and procedural omissions within the human resource system [10].

D. Prescriptive Improvement Mapping

The final phase involves translating the calculated technical gaps into formal, actionable, and prescriptive management recommendations. These recommendations are structured chronologically based on institutional priority and operational urgency, focusing heavily on eliminating the vulnerabilities identified across the DSS domain [6].

The improvement framework prioritizes designing missing standard operating procedures (SOPs), implementing formalized incident tracking matrices, securing user access controls, and establishing business continuity baselines [13]. These prescriptive guidelines provide a strategic roadmap for management to optimize SIMPEG services, protect personnel data assets, and sustain long-term digital public service efficiency.

Results

A. Observation and Interview

At this stage, interviews were conducted following the development of a questionnaire containing the Key Management Practices and Activities within the DSS domain. A detailed mapping of these activities within the DSS domain is presented in Table 2.

Table 2. Mapping Activity on Domain DSS

Process Name	Capability Level				Total Activity
	2	3	4	5	
DSS01 - Managed Operations	12	14	6	1	33
DSS02 - Managed Service Requests and Incidents	15	7	2	1	25
DSS03 - Managed Problems	9	8	5	1	23

DSS04 - Managed Continuity	23	12	4	2	41
DSS05 - Managed Security Services	26	18	5	0	49
DSS06 - Managed Business Process Controls	14	15	4	1	34
Total	99	74	26	6	205

Based on Table 2 above, the Deliver, Service, and Support (DSS) domain comprises a total of 205 activities. This total is distributed across several capability tiers, consisting of 99 activities for Capability Level 2, 74 activities for Capability Level 3, 26 activities for Capability Level 4, and 6 activities for Capability Level 5. The interview-based questionnaire process will systematically initiate from Capability Level 2.

B. Capability Level Assessment Results (DSS01 – DSS06)

The capability level assessment of IT governance in the SIMPEG system was conducted using the COBIT 2019 Process Assessment Model (PAM). The evaluation is based on questionnaire results using a Guttman scale, where each process is measured through Base Practice (BP) and Work Product (WP).
The capability score is calculated using the following formula:

Capability Score = (Total Achieved Activity / Total Activity) × 100%

DSS 01 – Managed Operations

Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 11 out of 12 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (11/12) x 100%
Capability Score = **91,67%**

According to the COBIT 2019 assessment guidelines, a compliance rate above 85% is categorized as **Fully Achieved (F)**. Therefore, the process has successfully satisfied the requirements for Capability Level 2, allowing the evaluation to proceed to Capability Level 3.

Based on the questionnaire recapitulation for Capability Level 3, this process successfully achieved 8 out of 14 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (8/14) x 100%
Capability Score = **57,14%**

Capability Level for this process has reached **57,14%**, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 4.

DSS 02 – Managed Service Requests dan Incidents

Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 11 out of 15 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (11/15) x 100%
Capability Score = **73,33%**

Capability Level for this process has reached **73,33%**, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 3.

DSS 03 – Managed Problems
Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 6 out of 9 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (6/9) x 100%
Capability Score = **66,67%**

Capability Level for this process has reached **66,67%**, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 3.

DSS 04 – Managed Continuity
Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 19 out of 23 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (19/23) x 100%
Capability Score = **82,6%**

Capability Level for this process has reached **82,6%**, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 3.

DSS 05 – Managed Security Services
Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 20 out of 26 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (20/26) x 100%
Capability Score = **76,92%**

Capability Level for this process has reached **76,92%**, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 3.

DSS 06 – Managed Business Process Controls
Based on the questionnaire recapitulation for Capability Level 2, this process successfully achieved 9 out of 14 available activities and the results is:

Capability Score = (Total Achieved Activity / Total Activity) × 100%
Capabality Score = (9/14) x 100%
Capability Score = **64,28%**

Capability Level for this process has reached 64,28%, which is categorized as **Largely Achieved**. Since it has not yet reached the Fully Achieved status (threshold >85%), the capability level evaluation cannot be extended to Level 3.

C. Gap Analysis (As-Is vs To-Be)

To optimize public services and secure personnel data asset compliance, the institution set a target capability framework of Level 3 (Defined Process) for all DSS sub-domains. Achieving Level 3 implies that all processes are structured, formally documented, and managed via organizational standards [4].

The quantitative gap analysis between the current governance baseline (As-Is) and the institutional target (To-Be) is summarized in Table 3.

Table 3. Capability Level and Gap Analysis Summary

Process Name	Current (As-Is)	Target (To-Be)	Gap
DSS01 - Managed Operations	3	3	0
DSS02 - Managed Service Requests and Incidents	2	3	1
DSS03 - Managed Problems	2	3	1
DSS04 - Managed Continuity	2	3	1
DSS05 - Managed Security Services	2	3	1
DSS06 - Managed Business Process Controls	2	3	1
Average	2,17	3,00	0,83

The data reveals an average current capability score of **2,17**, leaving an average governance gap of **0,83**. The capability gaps are observed in **DSS02, DSS03, DSS04, DSS05 and DSS06**. These structural gaps highlight that the SIMPEG platform operates without defined documentation guidelines, formal incident workflows, or robust business continuity safeguards.

D. Recommendations

To strengthen the implementation of IT governance improvements for enhancing SIMPEG services, the proposed recommendations are mapped directly onto the COBIT 2019 DSS sub-processes. This mapping ensures that each recommendation aligns with specific process practices, making the corrective actions more structured, measurable, and compliant with COBIT standards.

Table 4. Mapping Recommendations

No	Process Name	Description	Recommendation
1.	DSS01.01	Perform operational procedures	Develop and formalize SOPs for daily IT operations in SIMPEG
2.	DSS01.02	Manage outsourced IT services	Define roles and responsibilities for internal and external IT support
3.	DSS02.03	Verify, approve, and fulfill requests	Define workflows for request approval and resolution
4.	DSS02.04	Investigate, diagnose, and resolve incidents	Develop structured incident handling procedures
5.	DSS02.06	Track status and report	Implement dashboards and reporting mechanisms for incidents
6.	DSS03.01	Identify and classify problems	Create formal procedures for identifying recurring issues

No	Process Name	Description	Recommendation
7.	DSS03.02	Investigate and diagnose problems	Apply Root Cause Analysis (RCA) methods
8.	DSS03.03	Raise known errors	Develop a known error database
9.	DSS03.04	Resolve and close problems	Standardize problem resolution procedures
10.	DSS03.05	Perform proactive problem management	Implement preventive actions and continuous improvement
11.	DSS04.02	Maintain continuity strategy	Identify critical systems and define recovery priorities
12.	DSS04.03	Develop and implement continuity response	Establish Disaster Recovery Plan (DRP)
13.	DSS04.04	Exercise, test, and review plans	Conduct regular backup and recovery testing
14.	DSS04.05	Review, maintain, and improve plans	Perform periodic evaluation and updates of continuity plans
15.	DSS05.01	Protect against malware	Implement antivirus and endpoint protection systems
16.	DSS05.02	Manage network and connectivity security	Strengthen firewall and network security configurations
17.	DSS05.05	Manage physical access to IT assets	Secure physical access to servers and infrastructure
18.	DSS05.06	Manage sensitive documents and output devices	Protect confidential data and system outputs
19.	DSS05.07	Monitor security events	Implement security monitoring and logging systems
20.	DSS06.01	Align control activities embedded in business processes	Integrate IT controls with SIMPEG business processes
21.	DSS06.02	Control the processing of information	Implement validation and verification mechanisms
23.	DSS06.04	Manage errors and exceptions	Establish error handling and exception reporting procedures

Conclusion

This study evaluated the capability level of IT governance in the SIMPEG system using the COBIT 2019 framework, specifically focusing on the Deliver, Service, and Support (DSS) domain, which consists of DSS01 to DSS06. Based on the results, the assessment of the Deliver, Service, and Support (DSS) domain demonstrates that while the organization's current operational processes have generally achieved Capability Level 2, only the DSS01 sub-domain successfully advanced to Capability Level 3. Consequently, the remaining sub-domains specifically DSS02, DSS03, DSS04, DSS05, and DSS06 have not yet satisfied the institutional target gap of Capability Level 3. Based on these empirical findings, systematic improvements are fundamentally required to elevate the process compliance to a Fully Achieved status, thereby enabling the evaluation to proceed to subsequent capability tiers and minimizing the identified governance gaps. To bridge these capability gaps and enhance the overall reliability of the system, this study outlines 22 prescriptive action recommendations for the organization to implement.

References

[1] Firmansyah, D., Ridwan, M., Januriana, A. M., & Dongoran, A. (2024). Analisis Capability Domain DSS01 Menggunakan COBIT 2019 pada PT Solusi Finansialku Indonesia. *Jurnal Teknik Informatika Unika ST. Thomas (JTIUST)*, *09*(1).

[2] Ghanneson N., A., Amin, M., Putra, K., Nahampun, N., & Marsauli Sibarani, D. (2025). Analysis of Information Technology and Business Strategy Alignment in the Government Agency Personnel Management System Using the Luftman Model. *2nd International Conference on Islamic Community Studies (ICICS)*, 1178–1185. https://proceeding.pancabudi.ac.id/index.php/ICIE/index.

[3] Harjo, R. S. D. H., Kusrini, K., & Nasiri, A. (2023). Penentuan Domain Tata Kelola IT Pada Instansi Kepegawaian XYZ Menggunakan Kerangka Kerja Cobit 2019. *Jurnal Teknik Industri*, *9*(1), 31–43.

[4] ISACA. (2018). COBIT 2019 Framework Governance and Management Objectives. *Https://Www.Isaca.Org/Resources/Cobit.*, 302. https://www.isaca.org/resources/cobit.

[5] Manalu, A., Sitorus, Z., & Farta Wijaya, R. (2025). Evaluation of Information Technology Governance Using the Cobit 5 Framework at Putra Abadi University Langkat. *2nd International Conference on Islamic Community Studies (ICICS)*, 2955–2961. https://proceeding.pancabudi.ac.id/index.php/ICIE/index.

[6] Naibaho, E. B., & Cahyono, A. D. (2024). Information Technology Governance Analysis using COBIT 2019 Framework in Salatiga City Community and Civil Services. *Journal of Information Systems and Informatics*, *6*(2), 865–881. https://doi.org/10.51519/journalisi.v6i2.734

[7] Nugroho P. A, & Ambarwati A. (2025). Analisis Tata Kelola Teknologi Informasi di PT. Garam Menggunakan Framework COBIT 2019 Domain, Deliver, Services & Support. *TI Tersebut. Kata Kunci-COBIT*, *11*(1), 48–55.

[8] Permatasari, A. N., Sucipto, S., & Wardani, A. S. (2022). Analisa Kapabilitas Pengelolaan SIMPEG Menggunakan Framework COBIT 5 Domain DSS01 dan DSS03. *Journal of Informatic Engineering (JOUTICA)*, 34–43. https://jurnalteknik.unisla.ac.id/index.php/informatika.

[9] Safitri, A., Syafii, I., & Adi, K. (2021). Identifikasi Level Pengelolaan Tata Kelola SIPERUMKIM Kota Salatiga berdasarkan COBIT 2019. *Jurnal RESTI*, *5*(3), 429–438. https://doi.org/10.29207/resti.v5i3.3060.

[10] Syahputra, E., Iqbal, M., Farta Wijaya, R., & Nasution, D. (2024). EVALUATION OF INFORMATION TECHNOLOGY GOVERNANCE E-KINERJA SYSTEMS IN ASSESSING EMPLOYEE PERFORMANCE USING THE MODEL COBIT 2019 AT THE DISTRICT COMMINFO OFFICE WAS REALLY FUN. *Bulletin of Engineering Science, Technology and Industry*, *2*(3), 193–204. https://bestijournal.org.

[11] Utama, D. P., Muhammad, A. H., & Purwanto, A. (2023). AUDIT MANAJEMEN MASALAH TEKNOLOGI INFORMASI MENGGUNAKAN KERANGKA KERJA COBIT 2019 DOMAIN DSS03. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *8*(3), 839–846. https://doi.org/10.29100/jipi.v8i3.3946.

[12] Windasari, I. P., Rochim, A. F., Alfiani, S. N., & Kamalia, A. (2022). Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019. *Jurnal Sistem Informasi Bisnis*, *11*(2), 131–138. https://doi.org/10.21456/vol11iss2pp131-138.

[13] Yuan Mambu, J., Kaligis, J. E., Willar, A. M., & Adam, S. (2024). Analisa Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada Dinas Kominfo Provinsi Sulawesi Utara Analysis of Information Technology Governance Using the 2019 COBIT Framework at the North Sulawesi Province Communications and Information Service. *Journal of Computing Engineering, System and Science) e-ISSN*, *9*(2), 613–630. www.jurnal.unimed.ac.id.