ISSN: 2623-1662 (online), 2460-092X (printed)
DOI: https://doi.org/10.19109/jusifo.v11i2.31602
Vol. 11, No. 2 (2025), p.97-110

JUSIFO
JURNAL SISTEM INFORMASI

Research Article [OPEN ACCESS]

IT Governance Maturity Assessment of the BRAVO Application Using an Integrated COBIT 2019 and ITIL 4 Framework

Zahra Diva Putri Munaspin, Dwi Rosa Indah*, Habi Baturohmah, Ali Ibrahim, M. Rudi Sanjaya, M. Husni Syahbani

ABSTRACT

This study evaluates the maturity of IT governance supporting the BRAVO (BPKB Registration Vehicle Online) application at the Traffic Directorate of the South Sumatra Regional Police, a law enforcement institution delivering digital public services. An integrated evaluation approach combining COBIT 2019 and ITIL V4 frameworks was employed to assess governance and service management practices. Using design factor analysis, RACI-based respondent mapping, maturity level assessment, and gap analysis, the study focused on three key governance objectives: MEA03 (Managed Compliance with External Requirements), DSS02 (Managed Service Requests and Incidents), and DSS03 (Managed Problems). The findings indicate that MEA03 and DSS02 have achieved Maturity Level 3, reflecting structured and consistently implemented processes, while DSS03 remains at Maturity Level 2, indicating limited institutionalization of problem management practices. The gap analysis reveals significant maturity gaps between current and targeted levels, highlighting the need for governance strengthening, improved documentation, and enhanced analytical use of service data. This study demonstrates that integrating COBIT 2019 and ITIL V4 provides a coherent framework for bridging IT governance and service management, offering practical insights for improving digital public service delivery in law enforcement and other public sector organizations.

Keyword: COBIT 2019, IT governance maturity, ITIL V4

Received: October 24, 2025; Revised: December 19, 2025; Accepted: December 23, 2025

Corresponding Author: Dwi Rosa Indah, Department of Information System, Universitas Sriwijaya, Indonesia, indah812@unsri.ac.id
Authors: Zahra Diva Putri Munaspin, Department of Information System, Universitas Sriwijaya, Indonesia, 09031182227019@student.unsri.ac.id; Habi Baturohmah, Department of Information System, Universitas Sriwijaya, Indonesia, habibaturohmah@unsri.ac.id; Ali Ibrahim, Department of Information System, Universitas Sriwijaya, Indonesia, aliibrahim@unsri.ac.id; M. Rudi Sanjaya, Department of Information System, Universitas Sriwijaya, Indonesia, m.rudi.sjy@ilkom.unsri.ac.id; M. Husni Syahbani, Department of Information System, Universitas Sriwijaya, Indonesia, husnisyahbani@unsri.ac.id

1. INTRODUCTION

Indonesia's national digital transformation agenda has placed information technology at the core of public administration reform. This commitment was formally initiated through Presidential Instruction No. 3 of 2003 on E-Government Development and further institutionalized by Presidential Regulation No. 95 of 2018 concerning the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE), which provides a legal framework for integrated, transparent, and accountable digital governance. The adoption of SPBE across central and regional government institutions creates strategic opportunities to improve the quality, efficiency, and transparency of public service delivery (Gusman, 2024). This policy direction was reinforced by the Regulation of the Minister of Communication

and Informatics No. 16 of 2022, which mandates periodic Information and Communication Technology (ICT) audits to ensure compliance with national standards and service quality. Collectively, these regulatory instruments underscore the importance of effective IT management that is consistently aligned with organizational objectives, a condition that can only be realized through robust IT governance grounded in the principles of good governance (Hanif et al., 2020; Parera & Tambotoh, 2024).

In alignment with these national policies, the Indonesian National Police issued Regulation No. 9 of 2022 as an operational guideline for implementing SPBE within law enforcement institutions. This regulation directs all organizational units to systematically plan, develop, and manage integrated electronic services for both internal administration and public-facing services. One concrete manifestation of this policy is the BRAVO (BPKB Registration Vehicle Online) application developed by the Traffic Directorate (Ditlantas) of the South Sumatra Regional Police, which aims to digitalize Motor Vehicle Ownership Book (BPKB) services. This initiative reflects a broader effort to enhance public service quality through digital governance mechanisms (Ayunda et al., 2021). However, empirical findings from interviews with the Regident Sub-Directorate indicate that BRAVO continues to face significant challenges, including incomplete integration with the official Polri IT domain, limited interoperability with other systems, and unstable network infrastructure. These constraints not only hinder service optimization and regulatory compliance but also impede the realization of citizen-centric service delivery as mandated by SPBE principles (Rachmawati et al., 2022).

The persistence of these operational and technical issues points to underlying weaknesses in IT governance within Ditlantas Polda South Sumatra. Inadequate governance structures and oversight mechanisms limit the organization's ability to align IT initiatives with institutional objectives and public service expectations. As noted by Puspitaningrum et al. (2024), structured and standardized evaluation mechanisms are essential to identify governance gaps and guide systematic improvements. Without such evaluation, digital service initiatives risk becoming fragmented and misaligned, ultimately undermining public trust and organizational accountability. Therefore, a comprehensive and methodologically sound evaluation framework is required to strengthen IT governance performance and ensure sustained compliance with good governance principles.

Despite the extensive application of IT governance frameworks such as COBIT and ITIL in prior studies, existing research largely treats IT governance and IT service management as separate domains, particularly within public sector organizations. This separation is especially evident in law enforcement institutions implementing SPBE, where governance and service delivery are often evaluated independently. Such fragmented approaches fail to capture the interdependencies between governance structures, service management practices, and institutional objectives. As highlighted by Bagja et al. (2024) and Zaini et al. (2025) the absence of an integrated evaluation model limits objective performance assessment, weakens evidence-based decision-making, and ultimately reduces the effectiveness of public service delivery.

To address these limitations, this study adopts an integrated evaluation approach that combines the COBIT 2019 and ITIL V4 frameworks. COBIT 2019 offers a structured mechanism for assessing IT governance through design factors and capability maturity analysis (Francolla et al., 2022; ISACA, 2018a), while ITIL V4 emphasizes effective IT service management and value co-creation through service-oriented practices (Al-Ashmoery et al., 2024; ITIL Foundation, 2019). The integration of these frameworks enables a holistic assessment that simultaneously captures governance effectiveness and service delivery performance. Prior empirical studies have demonstrated that combining COBIT 2019 and ITIL V4 yields more comprehensive insights into governance and service gaps and supports the formulation of targeted and actionable improvement strategies (Nachrowi et al., 2020; Putra et al., 2022).

Accordingly, this study aims to evaluate the capability of IT governance processes at Ditlantas Polda South Sumatra using an integrated COBIT 2019 and ITIL V4 approach and to formulate evidence-based recommendations for improvement. Unlike prior research conducted in general governmental or corporate environments, this study specifically focuses on a law enforcement institution that delivers digital public services through the BRAVO application. In this context, IT governance is intrinsically linked to regulatory compliance, operational integrity, and public accountability, making rigorous evaluation particularly critical.

By applying COBIT 2019 design factor analysis and capability gap assessment within the SPBE implementation context, this study provides a context-specific evaluation of IT governance and IT service management practices within the Indonesian National Police environment. The findings are expected to offer practical insights into enhancing service continuity, governance effectiveness, and alignment between governance and service management functions. Ultimately, this research contributes to the development of an integrated and sustainable SPBE-based digital public service system within law enforcement institutions.

2. MATERIALS AND METHODS

2.1 Materials

This study was conducted at the Traffic Directorate (Ditlantas) of the South Sumatra Regional Police, with a specific focus on the BRAVO application. The research employed both primary and secondary data sources. Primary data were collected through semi-structured interviews and structured questionnaires administered to personnel within the Regident Sub-Directorate. Respondents were identified and selected based on the RACI (Responsible, Accountable, Consulted, and Informed) framework to ensure appropriate representation of governance roles.

Secondary data comprised organizational and technical documents relevant to the BRAVO system, including Standard Operating Procedures, system configuration reports, complaint and incident logs, and internal audit records. The research instruments consisted of interview guidelines and questionnaires developed in accordance with the COBIT 2019 framework to assess IT governance capability and maturity. A design factor analysis was conducted to identify critical governance and management processes, which subsequently informed the selection of relevant COBIT 2019 objectives for evaluation (Sukamto et al., 2021).

In addition, supporting materials included regulatory and institutional references, such as SPBE policies, internal IT governance guidelines of the Indonesian National Police, and prior audit documentation related to the BRAVO application. Collectively, these materials provided a comprehensive foundation for ensuring data accuracy, contextual relevance, and methodological validity throughout the research process.

2.2 Methods

This study employed a systematic, multi-stage research approach guided by the COBIT 2019 and ITIL V4 frameworks to evaluate IT governance and IT service management practices. The overall research flow is illustrated in Figure 1.

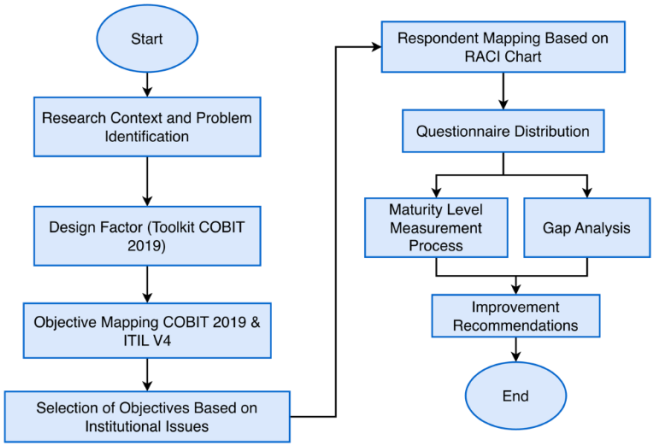

Figure 1. Research methods

The research process began with defining the research context and identifying key problems. At this stage, the organizational environment of Ditlantas Polda South Sumatra, as a law enforcement institution delivering digital public services through the BRAVO application, was examined to identify constraints, risks, and weaknesses in existing IT governance and service management practices. Within the COBIT 2019

framework, this phase corresponds to the initial focus area analysis, which prioritizes institutional issues as the foundation for subsequent evaluation.

Data obtained from observations, document reviews, and interviews with key stakeholders were analyzed to understand governance challenges and service delivery conditions and to support the identification of relevant design factors. The design factor analysis enabled a structured assessment of organizational characteristics, regulatory requirements, and operational needs, forming the basis for identifying and prioritizing COBIT 2019 governance and management objectives for improvement (Anastasia & Atrinawati, 2020; ISACA, 2018b; Morris et al., 2023). Subsequently, selected COBIT 2019 objectives were mapped to corresponding ITIL V4 practices to ensure that the evaluation comprehensively addressed both governance and service management dimensions. Objective selection was further refined based on institutional issues associated with the BRAVO application, with particular emphasis on compliance, incident management, and problem management.

Following the definition of evaluation objectives, respondents were mapped using the RACI chart to clarify roles and responsibilities in accordance with the Responsible, Accountable, Consulted, and Informed categories defined by COBIT 2019 (ISACA, 2018c). Structured questionnaires served as the primary instrument for assessing the capability levels of the selected objectives, using a capability scale ranging from Level 2 (Managed Process) to Level 5 (Optimizing). Capability assessment followed the COBIT 2019 capability model, in which achievement percentages were calculated for each process and interpreted using standardized rating criteria to determine capability levels.

A gap analysis was then conducted to identify discrepancies between the current capability level (as-is) and the expected target level (to-be), thereby revealing governance and service management gaps as well as factors constraining target attainment (Yusuf et al., 2024). Based on the results of the gap analysis, supported by interview findings and questionnaire data, targeted improvement recommendations were formulated. These recommendations, grounded in COBIT 2019 best practices, aim to mitigate risks, optimize IT resource utilization, and strengthen IT governance in support of digital transformation at Ditlantas Polda South Sumatra (Aflakhah & Soewito, 2023; Hidayah et al., 2024). In parallel, ITIL V4 service management practices were incorporated to reinforce service improvement recommendations, particularly in the areas of compliance management, incident management, and problem management.

3. RESULTS AND DISCUSSION

3.1 Research Context and Problem Identification

This study was situated within the Traffic Directorate (Ditlantas) of the South Sumatra Regional Police, a law enforcement institution responsible for delivering digital public services through the BRAVO application. Empirical evidence obtained from field observations and interviews with key stakeholders revealed several critical issues related to the IT governance and IT service management practices supporting the BRAVO system.

The results indicate that the BRAVO application has not yet been fully integrated into the official information technology domain of the Indonesian National Police. Consequently, the system remains dependent on third-party paid platforms, which limits institutional control over system development, operation, and governance. This condition introduces substantial governance risks, particularly with respect to regulatory compliance, system sustainability, and public accountability—core requirements for digital public services operating under the SPBE framework as mandated by Presidential Regulation No. 95 of 2018. Furthermore, unstable internet connectivity was identified as a major operational challenge, frequently disrupting system performance and causing service delays, thereby adversely affecting the quality and reliability of public service delivery.

Collectively, these issues underscore the need for a structured and systematic evaluation of IT governance and IT service management capabilities to ensure that the BRAVO application aligns with institutional objectives, regulatory mandates, and SPBE principles. The identified problems therefore provide the analytical foundation for the subsequent design factor analysis and inform the selection of relevant governance and management objectives for further capability assessment.

3.2 Design Factor Analysis Results

The design factor analysis was conducted to examine the organizational context and to adapt the implementation of IT governance in accordance with the COBIT 2019 framework. This analysis involved in-depth interviews with the Head of the BPKB Service Unit (BAUR SIE BPKB) at Ditlantas Polda South Sumatra, the organizational unit responsible for managing BPKB-related services. The interviews aimed to obtain first-hand insights into institutional conditions, operational challenges, and the strategic role of the BRAVO application in supporting digital public service delivery.

The findings of the design factor analysis were subsequently synthesized to determine the COBIT 2019 governance and management objectives most relevant to the organizational context. The consolidated results are presented in Figure 2, which summarizes the outcomes of the design factor assessment.

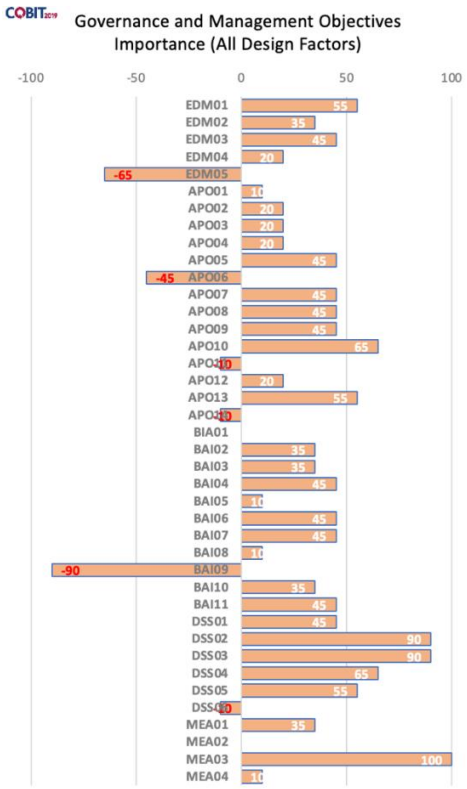

Figure 2. Design factor analysis

As illustrated in Figure 2, the analysis indicates that several COBIT 2019 governance and management objectives are particularly relevant to the implementation of the BRAVO application at Ditlantas Polda South Sumatra. Based on the integrated evaluation of all eleven COBIT 2019 design factors, five objectives were identified for further assessment: MEA03 (Managed Compliance with External Requirements), DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), DSS04 (Managed Continuity), and APO10 (Managed Vendors). These objectives exhibit strong alignment with the institution's regulatory compliance obligations, reliance on external service providers, and requirements for service reliability and continuity. Consequently, they were selected as the primary focus for evaluating the capability and maturity of IT governance and management practices within the organization.

3.3 Mapping of COBIT 2019 Objectives to ITIL V4 Practices

To ensure a comprehensive evaluation that extends beyond governance mechanisms alone, the selected COBIT 2019 objectives and their associated activities were systematically mapped to relevant service management practices defined in the ITIL V4 framework. This mapping was undertaken to establish alignment between IT governance processes and IT service management practices that are directly

applicable to the operational context of the BRAVO application at Ditlantas Polda South Sumatra. The results of the mapping exercise are presented in Table 1.

Table 1. Mapping of COBIT 2019 objectives to ITIL v4 practices

COBIT 2019		ITIL V4
MEA03	MEA03.01 Identify external compliance requirements	5.1.10 Risk management
	MEA03.02 Optimize response to external requirements	5.1.10 Risk management
	MEA03.03 Confirm external compliance	5.1.5 Measurement and reporting, 5.1.3 Information security management
	MEA03.04 Obtain assurance of external compliance	5.2.17 Service validation and testing, 5.1.2 Continual improvement
DSS02	DSS02.01 Define classification schemes for incidents and service requests	5.2.5 Incident management, 5.2.16 Service request management, 5.2.14 Service Desk
	DSS02.02 Record, classify and prioritize requests and incidents	5.2.5 Incident management, 5.2.16 Service request management, 5.2.14 Service Desk
	DSS02.03 Verify, approve and fulfil service requests	5.2.16 Service request management, 5.2.14 Service Desk
	DSS02.04 Investigate, diagnose and allocate incidents	5.2.5 Incident management, 5.2.14 Service Desk
	DSS02.05 Resolve and recover from incidents	5.2.5 Incident management
	DSS02.06 Close service requests and incidents	5.2.5 Incident management, 5.2.16 Service request management, 5.1.5 Measurement and reporting
	DSS02.07 Track status and produce reports	5.1.5 Measurement and reporting, 5.2.7 Monitoring and event management
DSS03	DSS03.01 Identify and classify problems	5.2.8 Problem Management
	DSS03.02 Investigate and diagnose problems	5.2.8 Problem Management
	DSS03.03 Raise known errors	5.2.8 Problem Management, 5.1.4 Knowledge Management
	DSS03.04 Resolve and close problems	5.2.8 Problem Management
	DSS03.05 Perform proactive problem management	5.2.8 Problem Management, 5.1.2 Continual Improvement
DSS04	DSS04.01 Define the business continuity policy, objectives and scope	5.2.12 Service continuity management, 5.2.1 Availability management
	DSS04.02 Maintain business resilience	5.2.12 Service continuity management, 5.2.1 Availability management, 5.2.7 Monitoring and event management
	DSS04.03 Develop and implement a business continuity response	5.2.12 Service continuity management, 5.2.1 Availability management
	DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)	5.2.12 Service continuity management
	DSS04.05 Review, maintain and improve the continuity plans	5.2.12 Service continuity management
	DSS04.06 Conduct continuity plan training	5.2.12 Service continuity management
	DSS04.07 Manage backup arrangements	5.2.7 Monitoring and event management
	DSS04.08 Conduct post-resumption review	5.2.12 Service continuity management, 5.2.7 Monitoring and event management
APO10	APO10.01 Identify and evaluate vendor relationships and contracts	5.1.13 Supplier management
	APO10.02 Select vendors	5.1.13 Supplier management
	APO10.03 Manage vendor relationships and contract	5.1.13 Supplier management
	APO10.04 Manage vendor risk	5.1.10 Risk management, 5.1.13 Supplier management
	APO10.05 Monitor vendor performance and compliance	5.1.13 Supplier management, 5.1.5 Measurement and reporting, 5.1.10 Risk management

As shown in Table 1, the selected COBIT 2019 governance and management objectives are mapped to multiple ITIL V4 practices, encompassing both general management practices and service management

practices. This mapping demonstrates a strong conceptual and operational alignment between the two frameworks, as they share comparable goals, control activities, and performance orientations. By integrating COBIT 2019 and ITIL V4 through this mapping, the evaluation framework ensures balanced coverage of strategic governance requirements and operational service management processes. Consequently, the assessment captures not only the effectiveness of IT governance structures but also the maturity of service delivery and support practices within the BRAVO system environment.

3.4 Selection of Objectives Based on Institutional Issues

This section explains the rationale for selecting specific COBIT 2019 objectives to address the research gap of this study, namely the evaluation of IT governance and IT service management practices within a law enforcement institution delivering digital public services through the BRAVO application. Based on the consolidated design factor analysis, five COBIT 2019 objectives were initially identified as relevant to the organizational context: MEA03, DSS02, DSS03, DSS04, and APO10. These objectives reflect key regulatory compliance requirements, operational challenges, and service continuity concerns associated with the implementation and operation of the BRAVO system.

To enable a focused, in-depth, and methodologically sound capability assessment, the evaluation scope was subsequently refined. This refinement was guided by several considerations, including the degree to which each objective directly addresses the most critical and recurring institutional issues, the availability and reliability of supporting empirical data, and the feasibility of conducting detailed evaluations within the defined research scope. As a result, three COBIT 2019 objectives—MEA03, DSS02, and DSS03—were selected for detailed capability assessment. These objectives specifically address regulatory compliance alignment, incident handling effectiveness, and problem management capability, which emerged as the most influential factors affecting the stability and effectiveness of BRAVO application services.

Conversely, DSS04 (Managed Continuity) and APO10 (Managed Vendors) were excluded from the detailed capability assessment. Although relevant at a strategic level, these objectives were assessed as less directly associated with the most critical recurring operational issues affecting the BRAVO application. In addition, limitations related to data availability and evaluation feasibility within the study's defined scope further constrained their inclusion. This selective focus ensures that the assessment remains analytically rigorous, contextually relevant, and empirically grounded.

The justification for selecting the final set of objectives, together with their corresponding institutional issues and evaluation focus areas, is summarized in Table 2. This table provides a transparent and structured overview of the alignment between institutional challenges and the selected COBIT 2019 objectives, thereby supporting methodological rigor, logical coherence, and transparency in the subsequent capability assessment stage.

Table 2. Selection of objectives based on institutional issues

	Reason for Selection	Focus Area
MEA03	The BRAVO application is not yet integrated with official Polri systems and relies on external paid services. This indicates a lack of regulatory alignment. The design factor analysis showed high external compliance requirements and strategic goals related to continuity and governance.	Evaluates alignment with external regulations and legal compliance for long-term sustainability.
DSS02	Frequent service disruptions and incident reports due to network instability and operational issues highlight the need for effective incident management. The design factor analysis emphasized the importance of responding to and resolving service requests efficiently, ensuring operational continuity.	Assesses the effectiveness of responding to and resolving service requests and incidents.
DSS03	Frequent service disruptions and incident reports due to network instability and operational issues reveal recurring problems that have not been fully addressed. The design factor analysis highlighted the importance of identifying the root causes of these problems and implementing long-term solutions.	Focuses on managing recurring problems and implementing preventive measures to improve service reliability.

3.5 Respondent Mapping Based on the RACI Framework

The distribution of questionnaires was guided by a respondent mapping process based on the RACI framework for each selected COBIT 2019 objective. The mapping prioritized respondents assigned to Responsible (R) and Accountable (A) roles, as these individuals are directly involved in the execution, oversight, and decision-making processes related to the evaluated objectives. This approach ensures that the assessment captures informed perspectives from key stakeholders with substantive authority and operational responsibility.

Based on the RACI mapping, respondents were identified for the selected objectives MEA03, DSS02, and DSS03. The detailed mapping of organizational roles and corresponding respondents for each objective is presented in Table 3, Table 4, and Table 5.

Table 3. Respondent mapping based on the RACI framework for MEA03

Role / Structure	Respondent
Chief Executive Officer; I&T Governance Board	Dirlantas
Chief Information Officer; Chief Operating Officer; Business Process Owner; Head of Development; Head of IT Operations; Head of IT Administration	Kasubdit Regident
Information Security Manager; Service Manager; Business Continuity Manager; Project Management Office; Privacy Officer	Kasi BPKB

Table 4. Respondent mapping based on the RACI framework for DSS02

Role / Structure	Respondent
Head of IT Operations; Chief Technology Officer; Business Process Owner; Head of Development	Kasubdit Regident
Service Manager; Information Security Manager	Kasi BPKB

Table 5. Respondent mapping based on the RACI framework for DSS03

Role / Structure	Respondent
Executive Committee	Dirlantas
Chief Information Officer; Chief Technology Officer; Head of Development; Head of IT Operations	Kasubdit Regident
Service Manager; Information Security Manager	Kasi BPKB

3.6 Maturity Level Measurement

Maturity level measurement was conducted based on questionnaire responses for the selected objectives, namely MEA03, DSS02, and DSS03. In this study, maturity was assessed using the process-based measurement scheme defined in COBIT 2019, which is conceptually derived from the Capability Maturity Model Integration (CMMI). The maturity level of each objective was determined by calculating the average score of all assessed activities across respondents to obtain an overall achievement score.

An activity was classified as fully achieved when its score exceeded 85% up to 100%. The assessment progressed to the next maturity level only if all activities at the current level were fully achieved. If any activity failed to meet this threshold, the assessment was terminated at that level. Accordingly, the final maturity level for each objective was defined as the highest level at which all required activities were fully achieved.

1. MEA03 (Managed Compliance with External Requirements)

The maturity level assessment results for MEA03 are summarized in Table 6. As shown in the table, activities at Maturity Level 2 achieved an average score of 96%, while Level 3 reached 100%, both

categorized as fully achieved. In contrast, activities at Level 4 achieved only 50%, which falls under partially achieved. Since Level 4 did not meet the minimum threshold for full achievement, the maturity level of MEA03 was determined to be at Level 3. This result indicates that compliance management processes are implemented in a structured and managed manner and are supported by organizational assets, although further consistency and continuous improvement are still required.

Document verification supported the questionnaire findings. Most compliance-related activities were adequately documented. Evidence for MEA03.01 included Service Policy Documents and Compliance Requirement Registers. MEA03.02 was supported by reports on service standard revisions and policy updates. For MEA03.03, evaluation reports and follow-up plans were available, although documentation related to installed license audits and insurance policy reports was incomplete. MEA03.04 was supported by compliance assurance reports and validation documentation. Overall, compliance management practices are generally well-documented, with minor gaps in audit-related records.

Table 6. Maturity level measurement of MEA03

Level	R1	R2	R3	Assessment Result	Rating Scale	Capability Level Achieved
1						
2	100	100	88	96%	F	
3	100	100	100	100%	F	Level 3
4	50	50	50	50%	P	
5						

2. DSS02 (Managed Service Requests and Incidents)

The maturity level assessment results for DSS02 are presented in Table 7. The results show that Maturity Level 2 achieved an average score of 90%, while Level 3 reached 93%, both classified as fully achieved. However, activities at Level 4 achieved only 50%, which is considered partially achieved. Consequently, the DSS02 process was assessed at Maturity Level 3. At this level, service request and incident handling processes are well-defined, systematically executed, and supported by organizational resources.

Supporting document analysis revealed that most documentation related to service request and incident management was available. DSS02.01 was supported by Service Standards and Configuration Repositories, although configuration status reports and problem classification schemes were incomplete. DSS02.02 was supported by consultation and complaint records, despite partial incident logs. DSS02.03 and DSS02.04 were evidenced by periodic complaint reports and evaluation and follow-up documentation, although some supporting incident symptom records were missing. DSS02.05 to DSS02.07 demonstrated comprehensive documentation related to incident resolution, user confirmation, and performance reporting. Overall, the DSS02 process is well-documented, with improvements required in incident logging completeness and supplementary reporting.

Table 7. Maturity level measurement of DSS02

Level	R1	R2	Assessment Result	Rating Scale	Capability Level Achieved
1					
2	87	93	90%	F	
3	100	86	93%	F	Level 3
4	50	50	50%	P	
5					

3. DSS03 (Managed Problems)

The maturity level assessment results for DSS03 are summarized in Table 8. The results indicate that Maturity Level 2 achieved an average score of 89%, which is categorized as fully achieved. However, Maturity Level 3 reached only 84%, which is classified as largely achieved and does not meet the minimum threshold for full achievement. Based on these results, the maturity level of DSS03 was determined to be at Level 2. This finding indicates that problem management objectives are met through standardized operational activities, although systematic root cause analysis and proactive problem prevention remain limited.

Document review showed that most problem management activities were supported by available documentation. DSS03.01 and DSS03.02 were supported by periodic consultation and complaint reports as well as evaluation and follow-up documentation. DSS03.03 and DSS03.04 demonstrated adequate documentation for incident resolution and problem closure, although known error databases and knowledge dissemination records were not available. DSS03.05 showed evidence of sustainable solution monitoring. Overall, DSS03 practices are implemented consistently, but improvements are required in error knowledge management and classification completeness.

Table 8. Maturity level measurement of DSS03

Level	R1	R2	R3	Assessment Result	Rating Scale	Capability Level Achieved
1						
2	89	89	89	89%	F	Level 2
3	88	88	75	84%	L	
4						
5						

3.7 Gap Analysis

A gap analysis was conducted to examine disparities between the current maturity levels (as-is) and the targeted maturity levels (to-be) of IT governance practices supporting the BRAVO application. This analysis aims to identify the extent to which existing practices align with the desired state of IT governance maturity. A visual representation of the gap analysis results is presented in Figure 3.

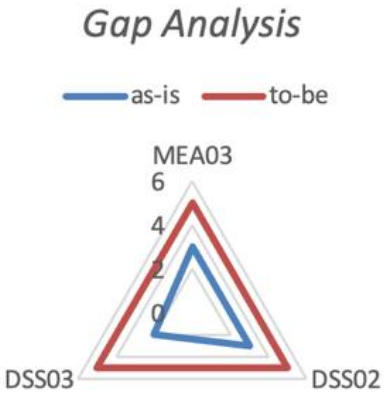

Figure 3. Gap analysis

As illustrated in Figure 3, the targeted maturity level for all three evaluated objectives is Level 5, reflecting stakeholders' aspirations to achieve optimal and continuously improving IT governance practices. However, the current maturity levels have not yet reached this target. Both MEA03 and DSS02 are currently positioned at Level 3, while DSS03 remains at Level 2. These results indicate a maturity gap of two levels for MEA03 and DSS02, and a three-level gap for DSS03, underscoring the need for targeted improvement initiatives to bridge these gaps.

3.8 Improvement Recommendations

The gap analysis reveals structural weaknesses in the maturity of IT governance and service management practices supporting the BRAVO application. The following recommendations are formulated to address these gaps by linking the identified maturity deficiencies with governance implications and strategic improvement directions. Rather than prescribing operational instructions, the recommendations emphasize governance strengthening, process institutionalization, and alignment between IT governance and service management, guided by COBIT 2019 principles and supported by relevant ITIL V4 practices.

1. **MEA03 (Managed Compliance with External Requirements)**

   The identified maturity gap in MEA03 indicates that compliance management remains predominantly reactive and insufficiently embedded within a formalized IT governance structure. This condition limits the organization's ability to anticipate regulatory changes and increases the risk of recurring non-compliance. To address this issue, compliance activities should be institutionalized as an integral component of IT governance, supported by systematic monitoring, structured evaluation, and risk-informed decision-making mechanisms. From an IT service management perspective, the integration of risk management, performance measurement, and service validation practices is essential to ensure that regulatory compliance is consistently aligned with service delivery and long-term organizational sustainability.

2. **DSS02 (Managed Service Requests and Incidents)**

   The maturity gap observed in DSS02 reflects limitations in leveraging incident and service request data beyond operational resolution. While service handling processes are in place, the absence of structured trend analysis and performance feedback constrains proactive service improvement and responsiveness. Strengthening this objective requires shifting from reactive incident handling toward analytical use of service data to support decision-making and service optimization. The adoption of ITIL V4 service management practices should therefore focus on enhancing analytical capability, service transparency, and cross-functional coordination, enabling more reliable and resilient digital public service delivery.

3. **DSS03 (Managed Problems)**

   The relatively low maturity level of DSS03 suggests that problem management practices are largely operational and corrective, with limited emphasis on root cause analysis, knowledge institutionalization, and organizational learning. This condition increases the likelihood of recurring incidents and undermines service stability. Improving this objective requires formalizing problem investigation processes, strengthening knowledge capture mechanisms, and embedding problem resolution outcomes into continuous improvement initiatives. By reinforcing problem management as a strategic governance function rather than a purely technical activity, the organization can enhance service reliability and reduce long-term operational risks.

Overall, these recommendations emphasize the need to transition from fragmented and reactive practices toward integrated, governance-driven IT management. Addressing the identified maturity gaps through structured governance mechanisms and analytically oriented service management practices is expected to support the sustainable improvement of the BRAVO application and strengthen the implementation of SPBE within the law enforcement context.

3.9 Discussion

This study examines the results of the IT governance evaluation at Ditlantas Polda South Sumatra through an integrated application of the COBIT 2019 and ITIL 4 frameworks. The findings indicate that MEA03 (Managed Compliance with External Requirements) and DSS02 (Managed Service Requests and Incidents) have achieved Maturity Level 3, reflecting structured implementation, standardized procedures, and consistent governance practices. At this level, governance processes are formally defined, monitored,

and aligned with organizational objectives, which is consistent with the principle of continual improvement emphasized in ITIL 4. These results corroborate prior studies reporting that systematic adoption of COBIT 2019 contributes to measurable improvements in IT governance maturity within public sector institutions. In contrast, DSS03 (Managed Problems) remains at Maturity Level 2, indicating that problem management activities are still largely operational and lack comprehensive institutionalization.

The integration of COBIT 2019 and ITIL 4 in this study provides added analytical value by linking governance-level objectives with operational service management practices. COBIT 2019 offers a robust structure for defining governance goals, capability targets, and compliance requirements, while ITIL 4 translates these objectives into practical service management activities. Through this integration, abstract governance requirements—such as regulatory compliance, incident responsiveness, and problem control—can be operationalized through concrete service practices, thereby strengthening alignment between strategic oversight and day-to-day service operations.

From a practical standpoint, this integrated approach enhances the interpretability and applicability of the evaluation results. COBIT 2019 enables systematic assessment of maturity levels and identification of governance gaps across key domains, including compliance, incident handling, and problem management. By mapping these objectives to corresponding ITIL 4 practices, governance findings can be directly associated with operational activities such as incident resolution, service request fulfillment, and problem investigation. This linkage facilitates the translation of governance assessment outcomes into service-oriented improvement strategies, ensuring that recommendations are both actionable and aligned with operational realities.

Despite these advantages, the combined use of COBIT 2019 and ITIL 4 requires careful methodological consideration. Differences in conceptual focus, terminology, and structural orientation between the two frameworks necessitate clear interpretative alignment to avoid inconsistencies between governance objectives and service management practices. Moreover, the effective application of ITIL 4 practices depends heavily on the maturity of existing processes and the availability of reliable documentation. In public sector and law enforcement contexts, where formal procedures and accountability are critical, limited documentation and uneven process standardization may constrain the effectiveness of framework integration.

Overall, the findings demonstrate that integrating COBIT 2019 and ITIL 4 can effectively bridge the gap between IT governance and IT service management in the delivery of digital public services. This integration enhances accountability, supports service reliability, and promotes continuous improvement within SPBE-based service environments. At the same time, the identified limitations underscore the importance of strengthening documentation practices and further institutionalizing process standards to fully realize the benefits of integrated governance and service management frameworks in law enforcement institutions.

4. CONCLUSION

This study evaluated the maturity level of IT governance supporting the BRAVO application at Ditlantas Polda South Sumatra through an integrated application of the COBIT 2019 and ITIL V4 frameworks. The assessment focused on three key governance objectives: MEA03 (Managed Compliance with External Requirements), DSS02 (Managed Service Requests and Incidents), and DSS03 (Managed Problems). The results show that MEA03 and DSS02 have achieved Maturity Level 3 (Defined), indicating that governance and service processes in these domains are formally documented and consistently implemented. In contrast, DSS03 remains at Maturity Level 2 (Managed), suggesting that problem management practices are operational but not yet fully institutionalized, particularly with respect to documentation completeness, root cause analysis, and preventive mechanisms. The gap analysis further revealed maturity gaps ranging from two to three levels, underscoring the need for targeted improvements, including stronger system integration, enhanced documentation practices, capability development through staff training, and more systematic monitoring and evaluation mechanisms.

Overall, the findings demonstrate that integrating COBIT 2019 and ITIL V4 provides a coherent and effective approach for assessing and improving IT governance maturity and service quality in public sector organizations. By linking governance objectives with service management practices, the integrated

framework supports greater alignment between strategic oversight and operational execution. Nevertheless, this study is subject to several limitations, as the evaluation was restricted to three governance objectives and conducted within a single law enforcement institution. Future research is therefore encouraged to extend the scope of analysis to additional COBIT and ITIL domains and to apply the integrated framework across multiple organizational contexts. Despite these limitations, this study contributes empirical evidence on the practical application of integrated IT governance and service management frameworks and offers insights into strengthening organizational performance, efficiency, and accountability in the delivery of digital public services.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Aflakhah, E., & Soewito, B. (2023). Assessing information security using cobit 2019 and iso 27001:2013 for developing a mitigation plan. *International Journal of Engineering Trends and Technology*, *71*(10), 223–237. https://doi.org/10.14445/22315381/IJETT-V71I10P221

Al-Ashmoery, Y., Chaabi, Y., Lekdioui, K., Al-Fuhaidi, B., Alwesabi, K., Haider, H., & Zaid, A. M. (2024). Impact of integrating lean, agile, and devops with itil4 framework for modern it service management. *1st International Conference on Emerging Technologies for Dependable Internet of Things, ICETI 2024*. https://doi.org/10.1109/ICETI63946.2024.10777262

Anastasia, P. N., & Atrinawati, L. H. (2020). Perancangan tata kelola teknologi informasi menggunakan framework cobit 2019 pada hotel xyz. *JSI: Jurnal Sistem Informasi (E-Journal)*, *12*(2), 2020. https://doi.org/10.18495/JSI.V12I2.26

Ayunda, R., Nertivia, N., Prastio, L. A., & Vila, O. (2021). Kebijakan online single submission sebagai e-government dalam mewujudkan good governance di indonesia. *Journal of Judicial Review*, *23*(1), 71–84. https://doi.org/10.37253/JJR.V23I1.4359

Bagja, A., Amri, Z., Imtihan, K., Rodi, M., & Rusniatun, S. Y. (2024). Enhancing public sector it governance through cobit 2019: a case study on service continuity and data management in the central lombok. *Journal of Information Systems and Informatics*, *6*(4), 2761–2776. https://doi.org/10.51519/JOURNALISI.V6I4.924

Francolla, G. B. R., Mandoya, R. G., Walangitan, M. D., Lompoliu, E., & Mambu, J. Y. (2022). Information technology governance analysis using the cobit 2019 framework at xyz institution. *CogITo Smart Journal*, *8*(2), 346–358. https://doi.org/10.31154/COGITO.V8I2.427.346-358

Gusman, S. W. (2024). Development of the indonesian government's digital transformation. *Dinasti International Journal of Education Management and Social Science*, *5*(5), 1128–1141. https://doi.org/10.38035/DIJEMSS.V5I5.2868

Hanif, A., Giatman, M., & Hadi, A. (2020). Evaluasi tata kelola teknologi informasi di dinas komunikasi dan informatika menggunakan framework cobit 5. *JST (Jurnal Sains Dan Teknologi)*, *9*(1), 94–101. https://doi.org/10.23887/JSTUNDIKSHA.V9I1.28401

Hidayah, N. A., Nurbojatmiko, N., Arfani, M. A., & Kusumaatuti, Y. A. (2024). Identifikasi tujuan tata kelola teknologi informasi plt fst uin jakarta menggunakan framework cobit 2019. *Journal of Applied Computer Science and Technology*, *5*(1), 90–97. https://doi.org/10.52158/JACOST.V5I1.770

ISACA. (2018a). *Cobit 2019 framework: introduction and methodology*. www.isaca.org.

ISACA. (2018b). *Designing an information and technology governance solution*. www.isaca.org.

ISACA. (2018c). *Implementing and optimizing an information and technology governance solution*. www.isaca.org.

ITIL Foundation. (2019). *ITIL 4 Edition* (1st ed.). TSO (The Stationery Office). https://www.axelos.com

Morris, G., Tangka, W., & Lompoliu, E. (2023). Information technology governance using the cobit 2019 framework at pt. pelindo tpk bitung. *CogITo Smart Journal*, *9*(2), 355–367. https://doi.org/10.31154/COGITO.V9I2.577.355-367

Nachrowi, E., Nurhadryani, Y., & Sukoco, H. (2020). Evaluation of governance and management of information technology services using cobit 2019 and itil 4. *Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(4), 764–774. https://doi.org/10.29207/RESTI.V4I4.2265

Parera, N. M., & Tambotoh, J. J. C. (2024). Measuring it governance capability at diskominfo salatiga using cobit 2019. *Sistemasi: Jurnal Sistem Informasi*, *13*(1), 324–334. https://doi.org/10.32520/STMSI.V13I1.3669

Puspitaningrum, A. C., Fitrani, L. D., & Sintiya, E. S. (2024). Systematic literature review: implementation cobit as a best practice of electronic based government system governance. *Sistemasi: Jurnal Sistem Informasi*, *13*(1), 335–345. https://doi.org/10.32520/STMSI.V13I1.3639

Putra, B., Jazman, M., Megawati, M., & Salisah, F. N. (2022). It governance audit at the kampar regency library and archives department using cobit 2019 and itil 4. *Jurnal Teknik Informatika (Jutif)*, *3*(6), 1591–1600. https://doi.org/10.20884/1.JUTIF.2022.3.6.406

Rachmawati, R., Anjani, D. F., Rohmah, A. A., Nurwidiani, T., & Almasari, H. (2022). Electronically-based governance system for public services: implementation in the special region of yogyakarta, indonesia. *Human Geographies*, *16*(1), 71–86. https://doi.org/10.5719/HGEO.2022.161.5

Sukamto, A. S., Novriando, H., & Reynaldi, A. (2021). Tata kelola teknologi informasi menggunakan framework cobit 2019 (studi kasus: upt tik universitas tanjungpura pontianak). *Jepin (Jurnal Edukasi Dan Penelitian Informatika)*, *7*(2), 210–218. https://doi.org/10.26418/JP.V7I2.47859

Yusuf, A., Saputra, W. A., & Jamilah, J. (2024). Capability gap analysis in it governance for a logistics company using cobit 2019. *Journal of Information Systems and Informatics*, *6*(3), 1804–1821. https://doi.org/10.51519/JOURNALISI.V6I3.832

Zaini, A., Widodo, A. P., Mutiara, D., & Nugraheni, K. (2025). Information system governance evaluation at diskominfo central java using cobit 2019 framework. *Scientific Journal of Informatics*, *12*(1), 67–76. https://doi.org/10.15294/SJI.V12I1.22883