Vifada Management and Social Sciences, E-ISSN 2987-1999

IT Governance Evaluation of Hospital Information Systems Using Framework: Case Study of RSUD Welas Asih

Muhammad Hanif Zahran [(1*)] *Sinung Suakanto* [(2)] *Basuki Rahmad* [(3)]

[(1,2,3)] *Telkom University, Bandung, Indonesia*

Received: 2026, 02,06 **Accepted**: 2026, 05,15
Available online: 2026, 06,30

* Corresponding author.
E-mail addresses: hanifzahran2@gmail.com

KEYWORDS

Keywords:
IT Governance; COBIT 2019; SIMRS; Hospital Information System; Capability Assessment; Data Triangulation; Service Reliability

Conflict of Interest Statement:
The author(s) declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

Purpose: This study evaluates the governance capability of the Hospital Management Information System (Sistem Informasi Manajemen Rumah Sakit/SIMRS) at RSUD Welas Asih using COBIT 2019 and formulates improvement directions to strengthen service reliability.

Research Design and Methodology: This study applies an evaluative case study with a mixed-method approach. Data were collected through a structured questionnaire completed by ten respondents from the SIMRS Installation, an interview with the Head of SIMRS Installation, direct observation, and limited document analysis. COBIT 2019 was used to assess selected APO, BAI, and DSS processes, while triangulation was applied to interpret questionnaire results against interview and documentary evidence.

Findings and Discussion: The questionnaire results show generally positive perceptions of SIMRS governance, especially in strategic alignment, user-driven development, and operational support. However, triangulation identifies improvement needs in periodic training, user adaptation after feature changes, change documentation, external system dependency, incident handling, manual fallback, data re-entry, BPJS claim validation, and infrastructure resilience.

Implications: The study recommends strengthening competency development, formal change logs, incident escalation, fallback procedures, data reconciliation, infrastructure continuity, and continuous governance monitoring.

Introduction

The rapid advancement of digital transformation in the healthcare sector has compelled hospitals, as public service institutions, to adopt information technology to improve operational efficiency, service quality, and decision-making effectiveness. In this context, the implementation of Hospital Management Information Systems (Sistem Informasi Manajemen Rumah Sakit/SIMRS) has become an essential component in supporting integrated healthcare service delivery. However, the success of SIMRS implementation is not solely determined by technological availability, but also by the extent to which governance and management processes ensure alignment between information technology initiatives and organizational strategic objectives (Saladdin & Handayani, 2025).

The increasing complexity of healthcare services requires hospitals to maintain information systems that are reliable, responsive, and capable of supporting operational continuity. Challenges related to process coordination, service disruption handling, change management, external system dependency, and organizational readiness often indicate governance limitations that reduce the effectiveness of information system utilization. (Saladdin & Handayani, 2025). These issues emphasize that technological implementation without structured governance evaluation may result in suboptimal system performance and limited contribution to institutional objectives.

Previous studies have demonstrated that information technology governance evaluation is essential for identifying capability gaps and improving organizational performance in healthcare institutions (Saladdin & Handayani, 2025). Evaluations using governance frameworks have shown that

many healthcare organizations still struggle with challenges related to management support, risk management, and business-IT alignment (Saladdin & Handayani, 2025). However, differences in institutional factors such as policy frameworks, infrastructure, and human resources significantly influence the outcomes of digital transformation initiatives (My & Linh, 2026).

RSUD Welas Asih has implemented SIMRS to support healthcare service operations and internal administrative processes across hospital units, including patient records, registration, service coordination, and integration with external healthcare systems. The hospital operates within a context of institutional accreditation, regulatory requirements, and user-driven system development. These conditions indicate that SIMRS is strategically important to hospital operations and must be governed not only for routine use but also for reliability during system changes, infrastructure incidents, and external service disruptions.

To address this issue, this study evaluates SIMRS governance at RSUD Welas Asih using the COBIT 2019 framework. The study focuses on selected governance and management objectives within the APO, BAI, and DSS domains to assess capability conditions, interpret governance gaps through triangulated evidence, and formulate structured improvement directions. Unlike a purely quantitative capability assessment, this study interprets questionnaire results alongside interview, observation, and document analysis to ensure that the evaluation reflects both perceived process achievement and actual governance conditions affecting SIMRS service reliability.

Literature Review

Hospital Information Systems (HIS), commonly implemented in Indonesia through the *Sistem Informasi Manajemen Rumah Sakit* (SIMRS), have become a fundamental technological infrastructure for supporting integrated healthcare service delivery. SIMRS facilitates the management of clinical, administrative, operational, and managerial information required to improve service effectiveness, patient safety, and institutional compliance with healthcare regulations (Kuswari, Gantino, & Maratis, 2024; Bendoly, Li, Smith, & Pavlou, 2025). The system integrates essential hospital functions, including patient registration, electronic medical records, pharmacy management, laboratory services, financial administration, human resources, and executive reporting. Through this integration, hospitals are expected to enhance operational efficiency, accelerate information accessibility, strengthen interdepartmental coordination, and support more accurate and timely managerial decision-making (Wijayakusuma & Rinawati, 2025). Despite these advantages, the effectiveness of SIMRS implementation depends not only on technological capability but also on the maturity of organizational governance. Hospitals frequently experience operational challenges such as service delays, inefficient workflows, inadequate incident management, and inconsistent information flows, which often reflect weaknesses in governance structures, process coordination, role accountability, and performance monitoring mechanisms (Amali, Katili, & Suhada, 2023).

Information technology has consequently evolved into a strategic enabler that supports organizational performance and healthcare service quality. Effective IT implementation contributes to operational efficiency, service continuity, regulatory compliance, risk mitigation, and evidence-based managerial decision-making (Okolo et al., 2024; Fatin, 2025). However, technology investments can only generate sustainable organizational value when they are aligned with institutional objectives through structured governance mechanisms. Strategic alignment ensures that information technology supports organizational priorities while enhancing clinical service continuity, administrative responsiveness, and public trust in healthcare delivery (Restrepo-Espinel, Moreno, & Aponte, 2024). Within this context, Information Technology (IT) governance provides the structures, processes, and relational mechanisms required to direct and control organizational information technology so that it consistently supports strategic objectives (Fattah, Saragih, & Setyadi, 2021). Unlike IT management, which focuses primarily on operational implementation and daily service execution, IT governance emphasizes strategic oversight, accountability, policy direction, risk optimization, value delivery, resource optimization, and performance evaluation (Asgarkhani, 2021). These governance principles are particularly important in healthcare organizations, where information systems operate within complex environments requiring reliable services, standardized

processes, and coordinated decision-making across multiple organizational units (Wulyatiningsih & Mambu, 2025).

Among the available IT governance frameworks, COBIT 2019 has emerged as one of the most comprehensive approaches for governing and managing enterprise information and technology. The framework provides structured guidance for aligning IT processes with organizational objectives through governance and management objectives, capability assessment mechanisms, and continuous improvement practices (Chukwurah, Ige, Adebayo, & Eyieyien, 2024). One of its key strengths is the incorporation of design factors, which enable organizations to customize governance systems according to their strategic priorities, operational characteristics, risk profiles, and regulatory requirements (Amali, Katili, & Suhada, 2023). Furthermore, the COBIT 2019 Process Assessment Model (PAM) facilitates systematic capability evaluation by measuring organizational processes against defined capability levels, allowing institutions to identify governance gaps, prioritize improvement initiatives, and establish measurable strategies for enhancing IT governance maturity (Puspitaningrum et al., 2025). Consequently, COBIT 2019 provides a robust foundation for evaluating and improving IT governance in hospitals seeking to optimize SIMRS implementation and achieve sustainable organizational performance.

Research Design and Methodology

This study employed an evaluative case study with a mixed-method approach to evaluate information technology governance within the SIMRS environment of RSUD Welas Asih. The case study approach was selected because the research focuses on one hospital context and seeks to understand governance practices within actual organizational, operational, and regulatory conditions. COBIT 2019 was used as the primary evaluation framework, while Design Science Research (DSR) was positioned only as a supporting approach for developing governance improvement recommendations as the final artifact of the study.

Data were collected through four sources: structured questionnaires, an interview with the Head of SIMRS Installation, direct observation, and limited document analysis. The questionnaire was distributed to ten respondents within the SIMRS Installation, including computer officers, operational service managers, information data officers, staff, and programmers. The questionnaire used the COBIT-based N, P, L, and F scale: Not Achieved, Partially Achieved, Largely Achieved, and Fully Achieved. Each selected process was assessed through process attributes up to Level 3, including PA 1.1, PA 2.1, PA 2.2, PA 3.1, and PA 3.2.

The selected COBIT 2019 processes were APO01, APO07, APO09, BAI01, BAI06, DSS01, DSS02, and DSS03. These processes were selected because they reflect the governance and management concerns most relevant to SIMRS reliability: governance framework, human resources, service management, development, change management, operations, incident handling, and problem management. The target capability level used in this study was Level 3 (Established Process), because the hospital requires processes that are not only performed and managed but also defined and consistently applied.

Data triangulation was applied to interpret the capability results. Questionnaire results were used to identify perceived process achievement, while the interview, observation, and document analysis were used to verify whether the practices were formally documented, consistently implemented, and capable of supporting SIMRS reliability under abnormal conditions. This triangulation was necessary because the questionnaire results were generally positive, whereas the interview revealed specific governance risks related to user adaptation, change documentation, external system dependency, manual fallback, data re-entry, claim validation, and infrastructure downtime.

Table 1. Research framework adaptation based on COBIT 2019

Variable	Code	Indicator	Major Reference
IT Governance Evaluation	X1.1	Strategic alignment of IT Governance	ISACA (2019)
	X1.2	Governance process capability level	
	X1.3	Service delivery effectiveness	
	X1.4	Monitoring and evaluation mechanisms	
Governance Improvement Recommendation	Y1.1	Gap identification	ISACA (2019)
	Y1.2	Process improvement priority	
	Y1.3	Governance enhancement recommendation	

***Source**: Research framework adaptation based on COBIT 2019*

The evaluation component in Table 1 concerns the assessment of governance capability in terms of strategic alignment, process capability, service delivery, and monitoring mechanisms. The recommendation component focuses on identifying governance gaps, prioritizing improvements, and developing governance enhancement directions to strengthen SIMRS service reliability.

To provide a comprehensive representation of the research process, a conceptual research framework was developed based on the COBIT 2019 governance framework and the supporting DSR logic for designing improvement recommendations. The framework illustrates the sequence of activities used to evaluate capability, identify gaps, interpret root causes, and formulate governance improvement recommendations. The original conceptual framework is retained in Figure 1.

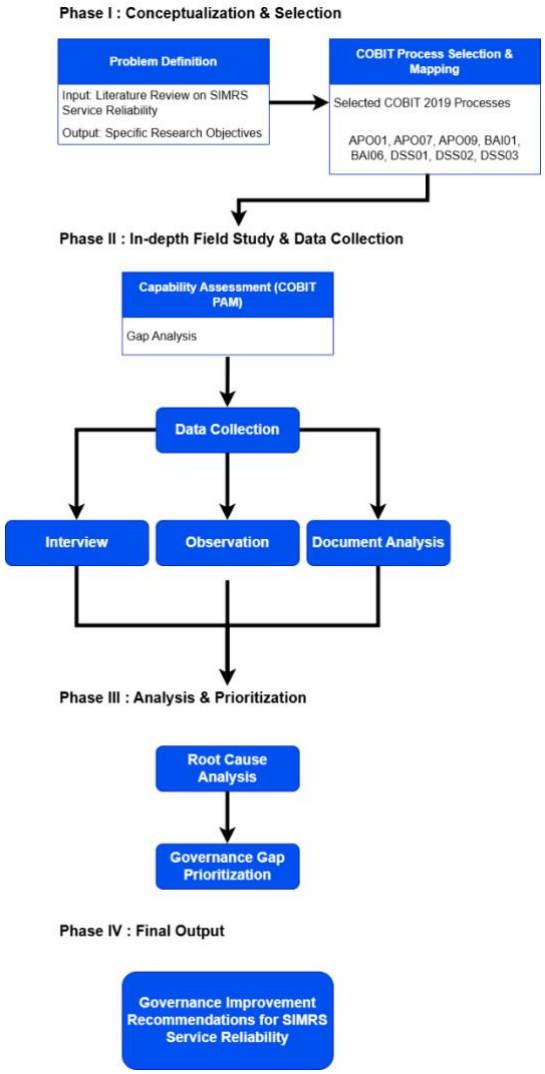

Figure 1. Research Framework for SIMRS Governance Evaluation and Improvement

***Source**: Author's elaboration based on COBIT 2019 (ISACA, 2019), Design Science Research (Peffers et al., 2007), and governance improvement concepts from NIST CSF 2.0 (NIST, 2024)*

As illustrated in Figure 1, the research is organized into four main phases. Phase I focuses on problem conceptualization and COBIT process selection. Phase II involves capability assessment and field data collection through questionnaires, interview, observation, and document analysis. Phase III analyzes capability gaps and root causes through triangulated evidence. Finally, Phase IV translates the findings into governance improvement recommendations. The figure remains unchanged because it represents the conceptual flow of the study, while the empirical interpretation is adjusted based on the actual field findings.

Findings and Discussion

Findings

This section presents the findings from the evaluation of SIMRS governance at RSUD Welas Asih using COBIT 2019. The results are based on questionnaire responses from ten SIMRS Installation respondents and were interpreted through triangulation with interview, observation, and document analysis. The questionnaire results were generally positive, with most responses falling into the Largely Achieved and Fully Achieved categories. However, several improvement areas emerged when the questionnaire findings were compared with interview and observational evidence.

1. Capability Assessment Results

The capability assessment was conducted across eight selected COBIT 2019 processes. The target capability level was Level 3 (Established Process). The current capability level was not determined solely from questionnaire scores; it was interpreted through triangulation. This approach was applied because several processes were perceived positively by respondents but still showed weaknesses in formal documentation, user readiness, external dependency handling, and reliability under abnormal conditions.

Table 2. Capability Assessment Results of Selected COBIT 2019 Processes

COBIT Processes	Process Description	Current Capability Level	Target Capability Level	Gap
APO01	Managed I&T Framework	3	3	0
APO07	Managed Human Resources	2	3	1
APO09	Managed Service Agreements	2	3	1
BAI01	Managed Programs and Projects	3	3	0
BAI06	Managed IT Changes	2	3	1
DSS01	Managed Operations	2	3	1
DSS02	Managed Service Request and Incidents	2	3	1
DSS03	Managed Problems	2	3	1

***Source**: Capability Assessment Results (2026)*

Table 2 shows that APO01 and BAI01 are relatively strong because SIMRS governance and development are aligned with hospital operations, user needs, hospital vision and mission, accreditation requirements, and regulatory expectations. In contrast, APO07, APO09, BAI06, DSS01, DSS02, and DSS03 remain at Level 2 because they are performed and managed in practice but require stronger formalization, documentation, continuity planning, and post-incident evaluation to consistently reach Level 3. The questionnaire results support this interpretation: for example, the periodic SIMRS training indicator in APO07 received five Partially Achieved and five Largely Achieved responses, indicating that training exists but is not yet fully structured or continuous.

2. Capability Assessment Results

Following the capability assessment, governance capability gaps were prioritized based on their potential impact on SIMRS service reliability. The prioritization results are presented in Table 3.

Table 3. Governance Gap Prioritization

COBIT Processes	Capability Gap	Impact on Service Reliability	Priority Level
APO01	0	Low	Low
APO07	1	High	High
APO09	1	High	High
BAI01	0	Low	Low
BAI06	1	Medium	High
DSS01	1	High	High
DSS02	1	Very High	Critical
DSS03	1	Very High	Critical

Source: *Research Analysis Results (2026)*

The prioritization analysis demonstrates that DSS02 and DSS03 represent critical improvement areas. These processes are directly related to incident handling, service recovery, data re-entry control, claim validation, and prevention of recurring problems. APO09 is also important because SIMRS reliability is affected by external systems such as JKN Mobile/BPJS and connectivity services, which are not fully controlled by the hospital.

3. Root Cause Findings

To understand the underlying factors contributing to the identified capability gaps, the questionnaire results were interpreted together with interview, observation, and document analysis. The main findings are summarized in Table 4.

Table 4. Summary of Root Cause Findings

COBIT Processes	Root Cause Findings
APO07	Periodic SIMRS training and user adaptation after new feature(s) implementation are not yet fully consistent across units.
APO09	SIMRS service reliability is affected by external system dependencies, particularly JKN Mobile/BPJS integration and connectivity services.
BAI06	Change documentation exists but is still mostly limited to before-after evidence rather than detailed change logs or release notes.
DSS01	Operational continuity can still be affected by infrastructure incidents, such as server harddisk replacement that cause temporary downtime.
DSS02	Incident handling for external disruption requires stronger escalation, manual fallback control, and re-entry procedures.
DSS03	Post-incident evaluation, data reconciliation, and BPJS claim validation controls need strengthening to prevent repeated operational and financial risks.

Source: *Interview, Observation, and Document Analysis Results (2026)*

Discussion

The discussion interprets the governance capability gaps identified during the assessment and explains how these gaps influence SIMRS service reliability. Rather than merely describing capability levels, this section examines the relationship between governance processes, organizational practices, external dependency, and service reliability outcomes. The discussion is based on the capability assessment results, governance gap prioritization, and root cause findings obtained from triangulated field evidence.

1. Governance Capability Gaps and SIMRS Service Reliability

The capability assessment indicates that RSUD Welas Asih does not face a fundamental absence of SIMRS governance. SIMRS has already been implemented across hospital units and supports important services, including patient records, registration, and internal administrative processes. Feature development is also based on user needs and aligned with the hospital vision, mission, accreditation

requirements, and regulatory demands. This explains why the questionnaire results were generally positive and why APO01 and BAI01 were interpreted as having reached the expected capability level.

However, triangulation shows that service reliability is challenged under abnormal conditions. These challenges include uneven user adaptation after new feature socialization, limited detail in change documentation, dependency on external systems such as JKN Mobile/BPJS and connectivity services, manual recording and re-entry risks during external disruption, BPJS claim validation risk, and infrastructure downtime during server component replacement. Therefore, the governance issue is not that SIMRS is unmanaged, but that several reliability-supporting mechanisms require stronger formalization and continuous evaluation.

Table 5. Summary of Governance Capability Gaps and Their Impact on SIMRS Service Reliability

COBIT Processes	Current Capability	Target Capability	Governance Gap	Potential Impact on SIMRS Service
APO01	Level 3	Level 3	Governance alignment is generally established	Supports strategic direction and user-driven SIMRS development
APO07	Level 2	Level 3	Periodic training and user adaptation are not fully structured	Some units may adapt slowly to new feature(s)
APO09	Level 2	Level 3	External dependency and service expectation control require strengthening	JKN/BPJS or connectivity disruption may affect registration and claims.
BAI01	Level 3	Level 3	Feature development is aligned with user needs and hospital priorities	Supports service improvement and regulatory readiness
BAI06	Level 2	Level 3	Change documentation is not yet detailed enough	Reduced traceability of feature changes and post-change learning
DSS01	Level 2	Level 3	Operational continuity procedures need strengthening	Temporary downtime may occur during infrastructure incidents or maintenance
DSS02	Level 2	Level 3	Incident handling for abnormal external disruptions is not yet fully formalized	Manual fallback and re-entry can increase service and data risks.
DSS03	Level 2	Level 3	Post-incident evaluation and reconciliation controls require improvement	Recurring issues and BPJS claim validation risks may persist

Source: *Developed by the author based on COBIT 2019 capability assessment (2026)*

Table 5 demonstrates that governance gaps are not evenly distributed across all processes. Strategic alignment and development prioritization are relatively strong, while reliability-related processes still require improvement. The findings indicate that SIMRS service reliability depends not only on internal system availability but also on the hospital's ability to manage user readiness, changes, incidents, external dependencies, and data reconciliation. This interpretation is consistent with the view that IT governance in healthcare must be understood as an integrated capability affecting operational continuity and service quality (Sumardiono, et al., 2026; Wulyatiningsih & Mambu, 2025)

To further explain how governance capability gaps influence service performance, the relationships identified during the assessment are illustrated conceptually in Figure 2.

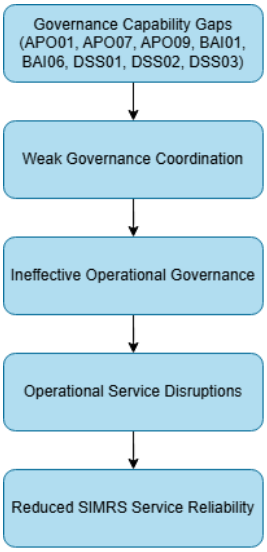

Figure 2. Relationship between Governance Capability Gaps and SIMRS Service Reliability
Source: *Developed by the author*

Figure 2 illustrates that governance capability gaps affect SIMRS service reliability through operational governance mechanisms. In the RSUD Welas Asih case, this relationship is reflected in external system disruption, manual fallback, re-entry risk, claim validation leakage, and downtime caused by infrastructure maintenance. The findings confirm that sustainable service reliability cannot be achieved solely by maintaining the application; it also requires structured governance of people, processes, changes, incidents, and external dependencies. (Sumardiono, et al., 2026).

Furthermore, the assessment demonstrates that governance-oriented processes, particularly APO01, APO07, and APO09, provide the organizational foundation for operational processes such as DSS01, DSS02, and DSS03. This relationship indicates that sustainable improvements in operational service performance cannot be achieved solely by strengthening technical operations. Instead, governance structures responsible for planning, organizational management, and service governance must first be improved to support consistent operational performance (AKINLEYE, George, & Ememe, 2025).

From the perspective of the first research question, these findings confirm that governance capability gaps influence SIMRS service reliability through interconnected organizational governance mechanisms rather than isolated process deficiencies. The capability assessment therefore functions as an organizational diagnostic tool that explains how governance weaknesses affect operational service performance and organizational effectiveness.

More importantly, the governance capability gaps identified in this phase establish the empirical foundation for the subsequent analysis presented in this study. While this section explains what governance deficiencies exist and how they affect SIMRS service reliability, the following sections investigate why these deficiencies occur through root cause analysis and subsequently formulate governance improvement priorities. These improvement priorities are then conceptually aligned with the NIST Cybersecurity Framework (CSF) 2.0 Govern Function to develop a structured governance improvement model that supports sustainable SIMRS service reliability (Malatji, 2025, p. 2).

2. Interpretation of Root Causes

Capability levels alone do not sufficiently explain why governance gaps occur. Therefore, the study interprets the organizational root causes based on interview, observation, and document analysis. The interpretation does not position accreditation-driven development as a weakness. Instead, alignment with user needs, hospital vision and mission, accreditation, and regulation is treated as a positive governance condition. The root causes focus only on weaknesses supported by field evidence.

To facilitate interpretation, the major governance capability gaps were synthesized into several organizational root cause categories, as presented in Table 6.

Table 6. Interpretation of Organizational Root Causes

Affected COBIT Processes	Governance Issue	Organizational Root Cause	Influence on Service Reliability
APO07	User readiness after feature(s) changes is uneven	Periodic training and competency evaluation are not fully structured across units	Users may require longer adaptation time after new feature(s) are launched
APO09, DSS02	Service reliability is affected by external dependency	JKN Mobile/BPJS integration and connectivity services are outside direct hospital control	External disruption can affect registration, claims, and patient service flow
BAI06	Change traceability is limited	Documentation is available but mainly in before-after form rather than detailed change logs	Change impact and post-implementation learning are harder to evaluate
DSS01, BAI06	Infrastructure maintenance can still cause downtime	Server component replacement is responsive but redundancy/failover planning need strengthening	Service availability may be interrupted during maintenance or incidents
DSS02, DSS03	Manual fallback and re-entry control need strengthening	Manual recording during downtime is not yet fully supported by formal reconciliation and claim validation controls	Data mismatch and BPJS claim leakage can create operational and financial risk(s)

Source: *Developed by the author based on interview, observation, and document analysis (2026)*

Table 6 shows that the most important root causes are related to governance formalization under abnormal conditions rather than the absence of SIMRS implementation. The severe external disruption case described in the interview demonstrates this point. When the external JKN/BPJS-related system experienced disruption, patient volume increased and the situation became difficult to control. Staff had to record patient data manually and later re-enter the data into the system. During this process, some patients passed through the service flow even though their claims could not later be processed, resulting in financial loss for the hospital. Although such severe incidents are now rare, the case demonstrates the need for stronger fallback procedures, data reconciliation, and claim validation controls. (Rohmanto, Wijana, Nurfadhilah, & Habiby, 2025)

To further illustrate the relationships among these organizational factors, the interpretation of root causes is conceptually summarized in Figure 3.

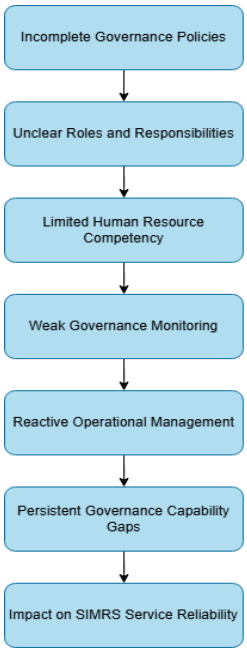

Figure 3. Organizational Root Causes of Governance Capability Gaps

Source: *Developed by the author*

Figure 3 should be interpreted in the context of the actual findings. The root causes do not suggest that the hospital lacks governance entirely. Instead, they show that several practices need stronger institutionalization: periodic training, formal change logs, external dependency handling, continuity planning, manual fallback control, data reconciliation, and post-incident review. These mechanisms are necessary to ensure that governance remains effective not only during routine operations but also during external disruption or infrastructure failure (Saladdin & Handayani, 2025).

This interpretation also explains the interdependence among the selected COBIT 2019 processes. Governance-oriented processes establish the organizational foundation that supports implementation and operational activities. Therefore, weaknesses identified in strategic governance are propagated throughout implementation and operational activities, reinforcing the persistence of governance capability gaps identified during the capability assessment (Mangoki, Manongga, & Iriani, 2024, p. 120).

From the perspective of the second research question, these findings demonstrate that governance capability gaps persist because organizational governance mechanisms have not been consistently institutionalized across strategic, tactical, and operational levels. Rather than representing isolated deficiencies within individual COBIT processes, the identified capability gaps reflect broader organizational governance challenges that require integrated governance improvement initiatives. Therefore, the interpretation of these organizational root causes provides the analytical basis for determining governance improvement priorities, which are presented in the following section and subsequently aligned with the Govern Function of the NIST Cybersecurity Framework (CSF) 2.0 to formulate a structured governance improvement model for enhancing SIMRS service reliability (Technology, The NIST Cybersecurity Framework 2.0, 2023, p. 4).

3. Governance Improvement Priorities

The interpretation of organizational root causes presented in the previous section demonstrates that governance capability gaps cannot be effectively addressed through isolated process improvements. Instead, sustainable improvements require governance initiatives that strengthen organizational structures, governance policies, human resource management, monitoring mechanisms, and continuous governance practices. Based on the capability assessment, governance gap prioritization, and root cause analysis, this section proposes governance improvement priorities designed to enhance the reliability of Hospital Management Information System (SIMRS) services. (Mangoki, Manongga, & Iriani, 2024, p. 112)

Rather than recommending improvements for individual COBIT processes separately, the proposed governance priorities consolidate multiple capability gaps into broader organizational governance initiatives. This approach enables the hospital to implement governance improvements systematically while maintaining alignment between strategic governance objectives and operational service delivery. (Mangoki, Manongga, & Iriani, 2024, p. 112).

Based on the capability assessment, prioritization, and root cause analysis, governance improvement should not be directed at replacing the existing SIMRS governance structure. Instead, improvement should strengthen the processes that support reliability during change, incident, infrastructure, and external dependency conditions. The proposed priorities are summarized in Table 7.

Table 7. Governance Improvement Priorities Based on Root Cause Analysis

Related COBIT Processes	Improvement Priority	Related Root Cause	Expected Contribution
APO07	Establish periodic SIMRS training and structured feature(s) socialization.	User adaptation after feature(s) changes is not fully consistent	Improve user readiness and reduce operational errors after new feature(s).
BAI06	Formalize changelogs, release notes, impact assessment, approval evidence, and post-implementation review.	Change documentation is still mainly before-after evidence	Improve traceability, accountability, and learning from system changes.

APO09, DSS02	Develop an external dependency register and incident escalation mechanism for JKN/BPJS and connectivity disruptions.	SIMRS reliability is affected by external systems outside direct hospital control.	Improve coordination and response to external service disruptions.
DSS01, DSS02	Standardize manual fallback procedures for high-volume service disruption conditions.	Manual recording and re-entry are required when external systems are down	Reduce service disruption and improve control during abnormal conditions.
DSS02, DSS03	Strengthen data reconciliation and BPJS claim validation after re-entry	Data mismatch and claim leakage can occur after manual fallback	Prevent financial loss and improve data reliability after incidents.
DSS01, BAI06	Improve infrastructure resilience through maintenance planning, backup verification, redundancy, and failover preparation.	Server component replacement caused temporary downtime.	Improve service continuity during maintenance and infrastructure incidents.
All selected processes	Institutionalize continuous governance monitoring and post-incident / post-change evaluation	Governance practices need consistent documentation and evaluation	Support sustainable improvement toward LEVEL 3 Capability.

Source: *Developed by the author based on capability assessment and root cause analysis (2026)*

Table 7 demonstrates that improvement priorities extend beyond increasing capability scores. Each recommendation directly addresses a root cause identified through triangulation. The recommendations are designed to preserve existing strengths, such as alignment with hospital vision, mission, accreditation, regulation, and user needs, while strengthening governance controls that support reliability during disruptive conditions. (Mangoki, Manongga, & Iriani, 2024, p. 112)

To further illustrate the relationship between governance priorities and organizational improvement, Figure 4 presents the proposed governance improvement model developed in this study.

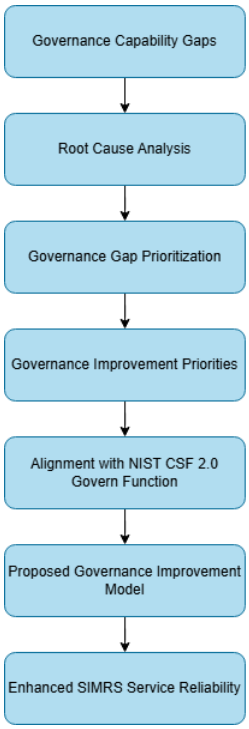

Figure 4. Proposed Governance Improvement Model for SIMRS Service Reliability
Source: *Developed by the author*

Figure 4 illustrates the governance improvement strategy proposed by this study. The model integrates COBIT 2019 capability assessment with root cause analysis to establish governance

improvement priorities. These priorities are aligned conceptually with the Govern Function of the NIST Cybersecurity Framework (CSF) 2.0, which provides guidance for governance structures, roles, policy management, oversight, and continuous improvement. (Technology, The NIST Cybersecurity Framework 2.0, 2023, p. 14). Rather than replacing COBIT 2019, the NIST CSF 2.0 Govern Function complements the capability assessment by providing strategic guidance for implementing governance improvements that are sustainable and adaptable to organizational needs (Technology, The NIST Cybersecurity Framework 2.0, 2023, p. 14).

The alignment between COBIT 2019 and the NIST CSF 2.0 Govern Function enables governance improvement recommendations to move beyond process-level corrections toward organization-wide governance enhancement. While COBIT 2019 identifies what governance capabilities require improvement (Annisa & Sulastri, 2023), the Govern Function of NIST CSF 2.0 provides guidance on how governance mechanisms should be strengthened through policy establishment, governance accountability, organizational oversight, and continuous governance evaluation (Technology, The NIST Cybersecurity Framework (CSF) 2.0, 2023, p. 22). Consequently, the proposed governance improvement model supports not only the achievement of higher governance capability levels but also the development of resilient governance practices capable of sustaining SIMRS service reliability over time.

From the perspective of the third research question, the proposed governance improvement model demonstrates that effective governance enhancement should be implemented through an integrated governance strategy encompassing organizational governance structures, human resource development, operational governance standardization, and continuous governance monitoring. This integrated approach ensures that governance improvements address the organizational causes of capability gaps rather than merely improving individual assessment scores. Accordingly, the proposed model provides practical guidance for hospitals seeking to strengthen SIMRS governance while enhancing service reliability and supporting long-term organizational resilience.

Conclusion

This study evaluated the governance capability of SIMRS at RSUD Welas Asih using COBIT 2019. The results show that SIMRS governance is generally positive in routine operations. The system supports hospital units, aligns with user needs, and is developed according to hospital vision, mission, accreditation, and regulatory expectations. This condition explains the generally positive questionnaire results, especially in governance alignment, user-driven development, and operational support.

However, triangulation with interview, observation, and document analysis shows that several areas still require improvement. The most important findings relate to uneven user adaptation after new feature socialization, limited detail in change documentation, dependency on external systems such as JKN/BPJS and connectivity services, manual fallback and re-entry risks during external disruption, BPJS claim validation risk, and infrastructure downtime during server component replacement. These findings indicate that the main governance challenge is not the absence of SIMRS implementation, but the need to strengthen formal governance mechanisms that support service reliability under abnormal conditions.

The study contributes to academic and practical understanding by demonstrating that COBIT 2019 capability assessment should be interpreted through triangulated evidence rather than questionnaire scores alone. From a practical perspective, the study recommends strengthening periodic training, change logs and release notes, incident escalation, manual fallback procedures, data reconciliation, claim validation controls, infrastructure resilience, and continuous governance monitoring. These recommendations are intended to support RSUD Welas Asih in moving toward more consistent Level 3 governance capability while preserving existing governance strengths.

This study is subject to limitations. First, the research was conducted as a single case study at RSUD Welas Asih, so findings may not be directly generalizable to other hospitals. Second, the questionnaire was limited to ten respondents from the SIMRS Installation, which reflects internal

governance perception rather than the perception of all hospital users. Third, document analysis was limited to documents made available during fieldwork. Future studies may expand the respondent group to clinical and administrative units, include broader documentary evidence, compare multiple hospitals, and evaluate the implementation of the proposed governance improvement model.

Acknowledgment

The author would like to express sincere gratitude to all individuals and institutions who contributed to the completion of this research. Special appreciation is extended to the Head of SIMRS Instalation for their continuous guidance, constructive feedback, and valuable academic insights throughout the research process. The author also gratefully acknowledges the management and staff of RSUD Welas Asih for their cooperation, participation, and support during the data collection process. Finally, the author would like to thank Telkom University and all parties who provided encouragement and support, directly or indirectly, in the completion of this study.

References :

Akinleye, O., George, O., & Ememe, J. (2025). Strategic role of corporate governance on organizational performance in the oil and gas industry in Nigeria. *Journal of Research in Business and Management, 13*(8), 7–18. https://doi.org/10.35629/3002-13080718

Amali, L., Katili, M., & Suhada, S. (2023). Core model of information technology governance system design in local government. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 21*(4), 750–758. https://doi.org/10.12928/telkomnika.v21i4.24287

Annisa, T., & Sulastri, H. (2023). Analysis of information technology governance of the Tasikmalaya City Manpower Service using the COBIT 2019 framework. *International Journal of Applied Information Systems and Informatics, 1*(1). https://doi.org/10.37058/jaisi.v1i1.8989

Asgarkhani, M. (2021). The internet, the cloud, and information technology governance. *International Journal for Applied Information Management, 1*(1). https://doi.org/10.47738/ijaim.v1i1.5

Bendoly, E., Li, M., Smith, J., & Pavlou, P. (2025). Operational process and agency considerations in managing emerging technologies in healthcare. *Journal of Operations Management, 72*(2), 164–175. https://doi.org/10.1002/joom.70029

Chukwurah, N., Ige, A., Adebayo, V., & Eyieyien, O. (2024). Frameworks for effective data governance: Best practices, challenges, and implementation strategies across industries. *Computer Science & IT Research Journal, 5*(7), 1666–1679. https://doi.org/10.51594/csitrj.v5i7.1351

Fatin, M. (2025). Optimizing strategy and outcomes: The role of IT investment and business analytics in business performance and healthcare. *Pacific Journal of Business Innovation and Strategy, 2*(4), 100–109. https://doi.org/10.70818/pjbis.v02i04.0121

Fattah, A., Saragih, H., & Setyadi, R. (2021). Determinants of the effectiveness of information technology governance and IT performance in higher education institutions: A conceptual framework. *International Journal of Science, Technology & Management, 2*(1), 36–47. https://doi.org/10.46729/ijstm.v2i1.135

Kuswari, M., Gantino, R., & Maratis, J. (2024). Maximizing healthcare service information systems: Understanding the influence of integration on efficiency. *ADI Journal on Recent Innovation, 6*(2), 108–117. https://doi.org/10.34306/ajri.v6i2.1145

Malatji, M. (2025). A cybersecurity AI agent selection and decision support framework. *arXiv*. https://doi.org/10.48550/arXiv.2510.01751

Mangoki, W., Manongga, D., & Iriani, A. (2024). IT governance design in XY University using the COBIT 2019 framework. *Jurnal Sistem Informasi Bisnis, 14*(2), 111–122. https://doi.org/10.21456/vol14iss2pp111-122

My, D., & Linh, H. (2026). Digital transformation and hospital operational efficiency: Global evidence and emerging lessons from Vietnam. *European Modern Studies Journal, 9*(6), 384–394. https://doi.org/10.59573/emsj.9(6).2025.26

National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Okolo, C., Ijeh, S., Arowoogun, J., Adeniyi, A., & Omotayo, O. (2024). Reviewing the impact of health information technology on healthcare management efficiency. *International Medical Science Research Journal, 4*(4), 420–440. https://doi.org/10.51594/imsrj.v4i4.1000

Puspitaningrum, A., Heri, S., Hafidz, M., Nurhadi, M., & Ananda, N. (2025). Evaluation of information technology governance at XYZ Bondowoso Hospital using COBIT 2019 and ITIL V4. *Teknika, 14*(2), 311–319. https://doi.org/10.34148/teknika.v14i2.1268

Restrepo-Espinel, G., Moreno, M., & Aponte, J. (2024). Business–IT alignment maturity diagnosis of a health organization using Luftman's SAM model. *Ingeniería e Investigación, 44*(2). https://doi.org/10.15446/ing.investig.101231

Rohmanto, R., Wijana, M., Nurfadhilah, S., & Habiby, M. (2025). Pengukuran tingkat maturity tata kelola sistem informasi rumah sakit dengan menggunakan framework COBIT versi 4.1. *INTERNAL: Information System Journal, 8*(2), 221–230. https://doi.org/10.32627/internal.v8i2.1872

Saladdin, I., & Handayani, P. (2025). Information technology governance implementation challenges in healthcare facilities: A systematic literature review. *SAGE Open, 15*(4). https://doi.org/10.1177/21582440251369322

Simatupang, S., & Fianty, M. (2023). Assessment of capability levels and improvement recommendations using COBIT 2019 for the IT consulting industry. *Jurnal Teknologi Terapan G-Tech, 7*(4), 1391–1400. https://doi.org/10.33379/gtech.v7i4.3141

Sumardiono, S., Supardi, S., Fitriani, S., Priyadi, W., Ismail, N., & Suryani, R. (2026). Unveiling IT governance effectiveness in e-Puskesmas using COBIT 2019. *Scientific Journal of Informatics, 13*(1). https://doi.org/10.15294/sji.v13i1.35868

Wijayakusuma, L., & Rinawati, R. (2025). Optimization of management information systems for improving hospital performance. *Jurnal Sosial dan Sains, 5*(7). https://doi.org/10.59188/jurnalsosains.v5i7.32319

Wulyatiningsih, T., & Mambu, J. (2025). IT governance maturity and business alignment: A COBIT 2019 evaluation at RSUD ODSK. *International Journal of Engineering Science and Information Technology, 5*(2), 248–255. https://doi.org/10.52088/ijesty.v5i2.822