Volume 12 Nomor 2, 2026, pp 182-190
ISSN: 2460-1799 P-ISSN: 1432-602743

Evaluating IT Governance Capability of SIT GMIM using COBIT 2019 Design Factors

Yoel Harmel Timothy Kumaat[1], Yohanes Andreas Robert Langi[2], Mahardika Inra Takaendengan[3], Dodisutarma Lapihu[4], Winsy Christo Deilan Weku[5], Stephano Caesar Wenston Ngangi[6]

[1,3,4,5,6] Sistem Informasi; Fakultas Matematika dan Ilmu Pengerahuan Alaml; Universitas Sam Ratulangi; Jl. Kampus UNSRAT Bahu, Malalayang, Kota Manado, Sulawesi Utara; Telp: (0431) 863886;
[2]Matematika; Fakultas Matematika dan Ilmu Pengerahuan Alaml; Universitas Sam Ratulangi; Jl. Kampus UNSRAT Bahu, Malalayang, Kota Manado, Sulawesi Utara; Telp: (0431) 863886;

[1]yoelkumaat13@gmail.com, [2]yarlangi@unsrat.ac.id, [3]mahardika@unsrat.ac.id, [4]dlapihu@unsrat.ac.id, [5]winsy_weku@unsrat.ac.id, [6]stephano.ngangi@unsrat.ac.id

* Korespondensi: e-mail: mahardika@unsrat.ac.id
Diterima: 22/07/2026 ; Review: 23/07/2026; Disetujui: 04/08/2026

ABSTRACT *– This study evaluates the IT governance capability of the SIT GMIM integrated information system using the COBIT 2019 framework. SIT GMIM supports church data management and administration at synod, regional, and congregation levels but has never undergone a formal IT governance evaluation. Using a mixed-method descriptive case study design, data were collected through questionnaires, semi-structured interviews, direct observation, and document review from SIT GMIM managers at the central synod level. Cobit 2019 performance management guides were used to evaluate capability levels for DSS01 to DSS06 (6 DSSI processes) and MEA01 to MEA04 (4 MEA processes). Gap analysis of current against target was undertaken. The DSS domain capability level was 1.17 on average (Level 1, Performed Process), the MEA domain capability level was 0.75 Level 1, Performed Process only. DSS02 reached Level 2 (Managed Process), while MEA04 remained at Level 0 (Incomplete Process). Gap analysis revealed DSS05 (Security Services) has the largest gap of 2 levels, while DSS03, DSS04, MEA02, MEA03, and MEA04 have gaps of 1 level. DSS01, DSS02, DSS06, and MEA01 achieved their targets. This research gives a first-hand, well-structured COBIT 2019 evaluation of a church IT system in Indonesia, setting a precedent for the enhancement of IT governance in religious groups. The main areas where improvement should be made through recommendations are: documenting processes, incident reporting, backup management, endpoint security, internal control review, compliance tracking, and the provision of assurance mechanisms.*

Keyword *– COBIT 2019; IT Governance; Design Factors; Capability Level; IT Audit; Religious Organization*

Evaluasi Kemampuan Tata Kelola TI SIT GMIM Menggunakan COBIT 2019 *Design Factor*

ABSTRAK *– Penelitian ini mengevaluasi kemampuan tata kelola TI sistem informasi terintegrasi SIT GMIM menggunakan framework COBIT 2019. SIT GMIM mendukung pengelolaan dan administrasi data gereja di tingkat sinode, regional, dan jemaah namun belum pernah menjalani evaluasi tata kelola TI secara formal. Dengan menggunakan desain studi kasus deskriptif metode campuran, data dikumpulkan melalui kuesioner, wawancara semi terstruktur, observasi langsung, dan telaah dokumen dari pengurus SIT GMIM tingkat sinode pusat. Panduan manajemen kinerja Cobit 2019 digunakan untuk mengevaluasi tingkat kemampuan untuk DSS01 hingga DSS06 (6 proses DSSI) dan MEA01 hingga MEA04 (4 proses MEA). Analisis kesenjangan arus terhadap target telah dilakukan. Tingkat kapabilitas domain DSS rata-rata 1,17 (Level 1, Performed Process), tingkat kapabilitas domain MEA 0,75 Level 1, Performed Process saja. DSS02 mencapai Level 2 (Proses Terkelola), sedangkan MEA04 tetap di Level 0 (Proses Tidak Lengkap). Analisis kesenjangan mengungkapkan DSS05 (Layanan Keamanan) memiliki kesenjangan terbesar sebanyak 2 level, sedangkan DSS03, DSS04, MEA02, MEA03, dan MEA04 memiliki kesenjangan sebanyak 1 level. DSS01, DSS02, DSS06, dan MEA01 mencapai targetnya. Penelitian ini memberikan evaluasi COBIT 2019 yang terstruktur dengan baik dan langsung terhadap sistem TI gereja di Indonesia, yang menjadi preseden bagi peningkatan tata kelola TI dalam kelompok keagamaan. Area utama dimana perbaikan harus dilakukan melalui rekomendasi adalah: proses pendokumentasian, pelaporan insiden, manajemen cadangan, keamanan titik akhir, tinjauan pengendalian internal, pelacakan kepatuhan, dan penyediaan mekanisme jaminan.*

Katakunci *– COBIT 2019; Tata Kelola TI; Faktor Desain; Tingkat Kapabilitas; Audit TI; Organisasi Keagamaan*

This is an open access article under the CC BY-SA license

Volume 12 Nomor 2, 2026, pp 182-190
ISSN: 2460-1799 P-ISSN: 1432-602743

1. INTRODUCTION

Religious organizations use integrated information systems to manage administration and service processes across multiple units. SIT GMIM is the integrated information system used by the central synod of GMIM to support administrative coordination, service delivery, and information management [1]. Because the system supports operational activities and decision making, its governance requires clear responsibility, documented procedures, and measurable performance. Without a formal assessment, managers cannot identify weak controls, prioritize improvements, or allocate limited information technology resources effectively [2].

COBIT 2019 provides a framework for assessing and improving the governance and management of enterprise information technology [3]. This method transforms the company's environment and requirements through several design elements into prioritized management and governance goals. Thereafter, process capability levels are used as metrics to assess selected processes. This work is centered on the Deliver, Service, and Support domain, besides Monitor, Evaluate, and Assess domain. DSS refers to the daily service delivery operational secure, and supportive aspects of the system. MEA involves monitoring, evaluation, and assurance of the system. Since the GMIM needs a system that runs smoothly and justifies its functioning to the synod, these domains apply to SIT GMIM.

Prior COBIT 2019 studies have applied DSS and MEA in several organizational contexts. Windasari et al. [4] found that audited processes were performed, but documentation and formal rules remained weak. Another study at a university faculty reported similar gaps between current and expected capability levels[5]. Assessments in other institutions also show that capability levels vary by process and by organizational context [6], [7], [8], [9].

However, most published evidence comes from universities, public agencies, and companies. Few studies examine church information systems. Religious organizations differ from those settings because they combine centralized administrative authority with a service-oriented mission and may operate with limited formal information technology management structures [10]. This context can affect how DSS and MEA practices are implemented and assessed. Therefore, an evaluation of SIT GMIM can show whether findings from secular organizations apply to a church setting and identify governance areas that require specific attention.

This study evaluates the information technology governance capability of SIT GMIM using COBIT 2019 design factors and the DSS and MEA domains. The assessment is limited to the central synod level. It does not evaluate congregation-level or regional-level users. The study examines the current capability level, the target capability level, the gap between them, and the factors that explain the gap. The results are used to formulate prioritized improvement recommendations.

The study contributes to information technology governance research by extending COBIT 2019 evidence to a religious organization and by examining DSS and MEA practices in a church information system. For practice, the study provides SIT GMIM managers with a capability baseline and identifies priority gaps.

2. METHODOLOGY AND MATERIALS

Research Design

This study employs a mixed-methods descriptive case study design. This approach integrates quantitative capability level assessments with qualitative contextual evidence. Case study methodology is appropriate for investigating complex, real-world IT governance practices within a bounded system [11]. The quantitative component applies the COBIT 2019 Performance Management model to score process capabilities. The qualitative component utilizes semi-structured interviews, direct observation, and document review to explain the underlying mechanisms of these scores [12], [13].

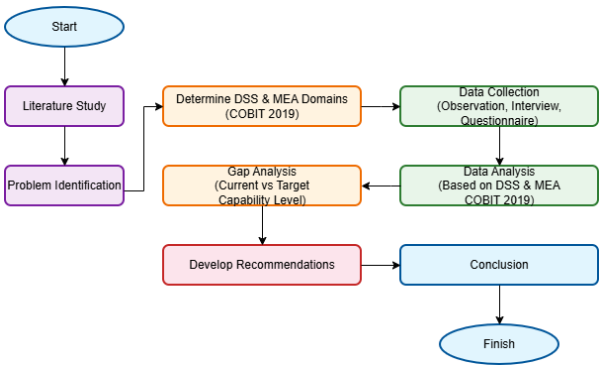

Figure 1. Research stages followed in this study.

Research Object

The research object is the IT governance of SIT GMIM at the central synod level. SIT GMIM is an integrated information system developed and maintained internally by GMIM to support administration, data management, and service delivery across synod, regional, and congregation levels. The central synod level was selected because it

holds the authority for governance rules, maintenance decisions, and resource allocation. Regional and congregation users possess access rights but do not participate in central IT governance and decision-making [2].

Stakeholder Identification

To identify relevant data sources, the study mapped stakeholder responsibilities using a RACI (Responsible, Accountable, Consulted, Informed) chart based on the GMIM organizational structure [14]. Table 1 presents the RACI mapping for the evaluated DSS and MEA processes.

Table 1. RACI Chart of SIT GMIM

Process	V. Chair	Div. Coord	Head	Team
DSS01	I	A	C	R
DSS02	I	A	C	R
DSS03	I	C	A	R
DSS04	I	A	C	R
DSS05	I	A	C	R
DSS06	I	C	A	R
MEA01	A	R	C	R
MEA02	A	R	C	R
MEA03	A	R	C	I
MEA04	A	R	C	R

The core central management and technical team responsible for SIT GMIM consists of exactly five individuals: the Division Coordinator, the Head of Section, two programmers, and one network administrator. Consequently, the sample size is five participants. While this sample is small, it represents the complete bounded population of central system managers and operators. In qualitative case study research, sampling prioritizes information richness and contextual boundaries over statistical generalization [13], [15]. These five informants possess comprehensive knowledge of the system's daily operations, incident handling, and governance practices.

Data Collection

Data were collected using four methods to ensure triangulation and construct validity [13].

a. Questionnaires

A preliminary fact-finding questionnaire was distributed to the SIT GMIM management team. The instrument contained 15 open-ended and categorical questions designed to collect factual data on the system profile, functional modules, user access levels, infrastructure facilities, and general incident handling procedures. Because this questionnaire collected objective system characteristics rather than latent psychological constructs or Likert-scale attitudes, statistical reliability metrics such as Cronbach's alpha are not applicable. Validity was established by cross-verifying the responses with internal documents and interview transcripts [13].

b. Semi-Structured Interviews

Three interview sessions were conducted with the Division Coordinator and the SIT GMIM technical team. The sessions lasted between 60 and 90 minutes and were conducted face-to-face at the GMIM Synod Secretariat. The interview protocol comprised 61 activity-specific questions mapped directly to the COBIT 2019 DSS (32 questions) and MEA (29 questions) practices. The full interview protocol is provided in Appendix A. The semi-structured format allowed participants to elaborate on their operational realities while ensuring all COBIT activity objectives were addressed. All sessions were audio-recorded and transcribed verbatim with participant consent.

c. Direct Observations

Non-participant observation was conducted over three days at the Synod Office. The researcher observed daily routines, including dashboard monitoring, user request handling via messaging applications, infrastructure checks, and internal coordination meetings. Field notes documented operational procedures, communication modes, and physical security arrangements.

d. Document Review

Internal documents were reviewed to corroborate interview and observation data. These documents included organizational charts, system manuals, backup logs, hardware inventories, meeting minutes, and user complaint records.

Data Analysis

Data analysis followed the COBIT 2019 Performance Management guidelines [8], [16], [17]. The procedure consisted of four steps.

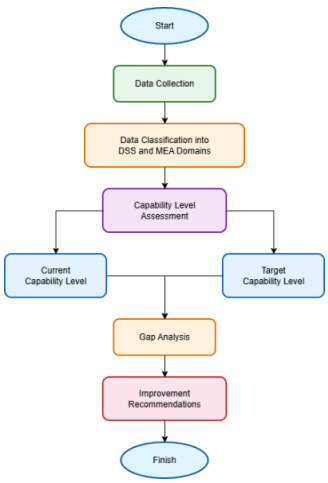

Figure 2. Performed data analysis procedure used in this study and presented the results.

Step 1: Data Classification and Mapping

Qualitative data from transcripts, field notes, and documents were classified according to the 10 evaluated COBIT 2019 processes (DSS01 to DSS06 and MEA01 to MEA04). Each piece of evidence was mapped to specific activity objectives within those processes.

Step 2: Capability Level Assessment

Each activity was scored on a scale from 0 to 5 based on the COBIT 2019 capability levels (Table 2). The scoring evaluated the presence and quality of evidence regarding execution, planning, standardization, measurement, and continuous improvement.

Table 2. Capability Level Scale (COBIT 2019).

CL	Name	Score Range
0	Incomplete Process	0.00 – 0.50
1	Performed Process	0.51 – 1.50
2	Managed Process	1.51 – 2.50
3	Established Process	2.51 – 3.50
4	Predictable Process	3.51 – 4.50
5	Optimising Process	4.51 – 5.00

The process capability level (CL_p) was calculated as the arithmetic mean of its constituent activity scores (CL_{ai}):

$$CL_p = \frac{\sum_{i=1}^{n} CL_{ai}}{n} \qquad (1)$$

Where n is the number of activities in that process. For example, DSS01 has five activities (DSS01.01–DSS01.05); the average of their scores gives the capability level for DSS01.

Step 3: Determination of Target Capability Level

Target capability levels were established using the COBIT 2019 Design Toolkit [6]. The toolkit maps organizational context, strategic importance, and management priorities to suggested target levels. The suggested targets were reviewed and validated with the Division Coordinator to ensure alignment with available resources and realistic organizational goals.

Step 3: Determination of Target Capability Level

The gap for each process was calculated as:

$$Gap = \text{TargetCL-CurrentCL} \quad (2)$$

A positive gap indicates the number of capability levels the process must advance to reach the target state. Processes with the largest gaps were prioritized for improvement recommendations.

Ethical Considerations

The research explained a bit about the study's purpose and participants' right to withdraw anytime without any negative consequences through a sheet given to them. They were given informed consent on paper before the interviews. All the transcripts with personal identities were kept in separate documents for analysis after the identities were removed from them. Only the research team knows the password to a system that holds the audio recordings and the transcripts.

Methodological Limitations

This study has specific limitations. First, it evaluates only the central synod management level, excluding the perspectives of regional and congregation users. Second, the single-case design limits statistical generalization to other religious organizations [15]. Third, the assessment covers only the DSS and MEA domains; other COBIT domains remain unevaluated. Finally, capability scoring relies on researcher judgment based on qualitative evidence, which introduces a degree of subjectivity mitigated only through data triangulation

3. RESULT AND DISCUSSION

Determination of Target Capability Levels

Target capability levels were established using the COBIT 2019 Design Toolkit and validated with the SIT GMIM Division Coordinator. The mapping considered the organizational strategy, risk profile, and resource constraints of the central synod. Table 3 presents the target capability levels and the rationale for each selected process.

Table 3. Target Setting Rationale.

Process	Target	Rationale
DSS01	1	Basic operational activities are already performed; target is to maintain them with better evidence/documentation.
DSS02	2	Incident handling already shows some management characteristics (Level 1.57); target is to formalise recording and tracking.
DSS03	2	Problem identification exists but lacks structured root-cause analysis and knowledge base; target is to manage problems proactively.
DSS04	2	Backup and recovery exist but without formal BCP/DRP; target is to establish documented continuity plans.

Process	Target	Rationale
DSS05	3	Security is critical due to sensitive membership data; target is to establish formal policies, endpoint security, and vulnerability monitoring.
DSS06	1	Controls are performed informally; target is to maintain them with basic evidence.
MEA01	1	Monitoring is performed via dashboard; target is to maintain with better reporting.
MEA02	2	Controls exist but lack self-assessment; target is to manage controls with periodic evaluation.
MEA03	2	Awareness of regulations exists; target is to formalise compliance tracking and documentation.
MEA04	1	No formal assurance exists; target is to establish basic evaluation mechanisms as a first step.

Current Capability Level Assessment

The assessment evaluated six DSS processes and four MEA processes based on interview transcripts, observation notes, and document reviews.

1. DSS Domain Results

In DSS, DSS02 (Managed Service Requests and Incidents) scored the highest 1.57 on the Scale, and is rated at the Level 2 (Managed Process). Handling incident shows the basic required management characteristics by impact-based priority, assigned responsibility. But it lacks of a formal ticket system which limit its scoring at Level 2. DSS04(Manged Continuity) and DSS05(Manged Security Services) have scores 0.75 and 0.86 respectively. Both of them are Level 1 rated but indicated weaknesses at some area. The score for DSS05 were zero at endpoint security (DSS05.03), Monitor issues like vulnerability (DSS05.07).

Table 4. DSS Domain Capability Level Results

Process	CL	Category
DSS01	1.00	Level 1(Performed Process)
DSS02	1.57	Level 2 (Managed Process)
DSS03	1.00	Level 1 (Performed Process)
DSS04	0.75	Level 1 (Performed Process)
DSS05	0.86	Level 1 (Performed Process)
DSS06	1.00	Level 1 (Performed Process)

Overall DSS Domain Capability Level. The average capability level for the DSS domain is calculated as:

$$CL_{DSS} = \frac{1+2+1+1+1+1}{6} = \frac{7}{6} = 1.17 \approx 1$$

2. MEA Domain Results

Within the MEA area MEA01 MEA02, and MEA03 scored 1.00, 1.00, and 0.75 respectively, This way earning them Level 1 status. MEA04 (Managed Assurance) obtained a score of 0.00 which resulted in a Level 0 (Incomplete Process) classification. The company does not have a separate assurance unit, its audit planning is not based on risks, and there are no formal assessment methods.

Table 5. MEA Domain Capability Level Results.

Process	CL	Category
MEA01	1.00	Level 1 (Performed Process)
MEA02	1.00	Level 1 (Performed Process)
MEA03	0.75	Level 1 (Performed Process)
MEA04	0.00	Level 0 (Incomplete Process)

Overall, MEA Domain Capability Level. The average capability level for the MEA domain is calculated as:

$$CL_{MEA} = \frac{1+1+1+0}{4} = \frac{3}{4} = 0.75 \approx 1$$

Table 6. Summary of Current Capability Levels

Domain	$\bar{x}$ CL	Category
DSS	1.17	Level 1 (Performed Process)
MEA	0.75	Level 1 (Performed Process)

Generally, the results reveal that the SIT GMIM's IT governance processes are performed on a fundamental operational level, yet these processes do not include management, documenting, and formalizing steps that are important to moving to high capability levels. In fact, this is true of all items, except DSS02, for which some signs of initial management activities (Level 2) were found. The biggest problem is MEA04 completely missing (Level 0).

Gap Analysis

The gap analysis compares the current capability levels with the agreed target levels to identify improvement priorities. Table 7 details the gap for each process.

Table 7. Gap Analysis Results

Process	Current CL	Target CL	Gap
DSS01	1	1	0
DSS02	2	2	0
DSS03	1	2	1
DSS04	1	2	1
DSS05	1	3	2
DSS06	1	1	0

Process	Current CL	Target CL	Gap
MEA01	1	1	0
MEA02	1	2	1
MEA03	1	2	1
MEA04	0	1	1

These four processes namely DSS01 DSS02 DSS 06 and MEA01 have reached their target level and their gap is zero. The lag in five other processes namely DSS03 DSS04 MEA02, MEA03 and MEA04 is of one level. DSS05 (Managed Security Services) exhibits the largest gap of two levels, requiring immediate intervention to reach the target Level 3.

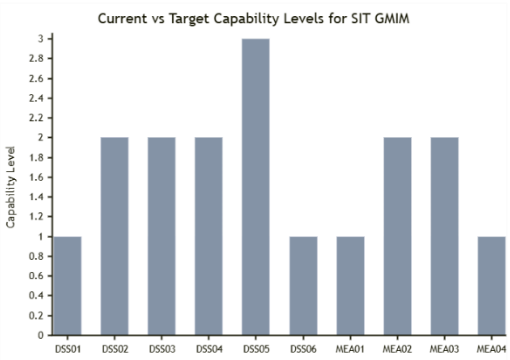

Figure 3. Current vs Target Capability Levels

Figure 3 visualizes the current versus target capability levels.

Discussion

IT Governance Maturity in a Religious Organizational Context

The overall capability levels for SIT GMIM cluster at Level 1 (Performed Process). The system operates and delivers basic services, but processes rely heavily on informal communication, individual memory, and reactive troubleshooting rather than documented standard operating procedures. This finding aligns with the broader tendency in resource-constrained organizations to execute IT activities informally [3].

The reliance on informal governance mechanisms in SIT GMIM stems directly from the structural characteristics of religious organizations. Unlike corporate entities, the central synod IT team operates with a minimal technical staff of three individuals and relies on decentralized volunteer operators at the regional and congregation levels. This structure limits the capacity for formal documentation and strict policy enforcement. Church administration prioritizes immediate service delivery and pastoral support over bureaucratic IT compliance [10]. Consequently, IT governance practices emerge organically to solve immediate problems rather than through top-down strategic planning.

The Security Deficit: Analyzing the DSS05 Gap

DSS05 (Managed Security Services) is the biggest capability gap in the analysis, needing two levels of improvement to reach a desired result. Besides using standard methods to protect the perimeter, like firewalls, antivirus software, and Role-Based Access Control (RBAC), there's no implementation of endpoint security management nor any form of systematic and ongoing vulnerability monitoring. This deficiency in security is Mainly alarming for the type of information the SIT GMIM processing system handles. The data includes the names and contact details of members, their payment donations, and their ministers' records. Based on Indonesia's Personal Data Protection Law (UU No. 27 Tahun 2022), the church as data controller is under a duty of law to protect the data [5].

There is a big issue at the church, which has been using mostly free and very basic security software. That's where the problem with security tools starts. The church isn't equipped with the kind of tools that detect weaknesses like vulnerability scanners or even a dedicated security staff. Besides that, they lack the budget for it. They handle security in a purely reactive manner, solving issues as and when a user complains or a system failure occurs. That's not how it should be; a church of any size should constantly be looking out for cybersecurity threats. The church needs to set up a policy of information security at the earliest stage and invest money in vulnerability discovery tools that have a low cost and are automated.

The Assurance Void: Explaining the MEA04 Baseline

MEA04 (Managed Assurance) scored 0.00, indicating that the process is entirely incomplete. Assurance requires an objective, independent evaluation of IT controls against established criteria. In the context of SIT GMIM, the individuals who design, operate, and maintain the system are the exact same individuals tasked with evaluating it. The central synod does not possess an internal IT audit department, and external IT audits are not commissioned due to budget constraints.

System evaluations currently occur only during annual synod meetings or when severe disruptions prompt leadership inquiries. These reactive discussions do not constitute formal assurance because they lack a defined scope, structured work programs, and independent reporting [3]. Establishing a Level 1 assurance capability does not require hiring external auditors immediately. The synod can initiate basic assurance by integrating formal IT quality reviews into the annual synod secretariat audit schedule and assigning a non-technical administrative officer to verify IT compliance checklists.

Cross-Sector Comparison and Theoretical Implications

The capability gaps identified in SIT GMIM share surface-level similarities with IT governance assessments in other sectors. Windasari et al. [4], [5] found that university faculties and engineering departments also stall at Level 1 due to missing documentation and unclear rules. Similarly, Wahyudi and Sutedi [19] identified poor documentation and weak internal controls in a postal service company.

Still, the root causes that explain these differences are quite different from one context to another. At educational institutions and governmental bodies, the reason for unstructured IT governance is mainly due to departmental isolation, highly sophisticated old systems, or conflicting goals between departments [20]. In religious organizations like GMIM, the informal governance is a direct adaptation to extreme resource limitations, volunteer reliance, and an organizational culture that values pastoral agility over administrative rigidity. This study extends COBIT 2019 theory by demonstrating that while the framework's capability metrics remain universally applicable, the root causes of capability deficits are highly context-dependent. In addition, conventional approaches to corporate problem-solving like employing specialized compliance officers or buying expensive enterprise governance software tend to be impractical solutions for church-related organizations. Rather than these methods, solutions should utilize already established church reporting systems and inexpensive digital technologies.

Practical Implications for Church IT Management

The findings provide SIT GMIM managers with a prioritized baseline for IT governance improvement. Processes with a zero gap (DSS01, DSS02, DSS06, MEA01) require only the formalization of existing practices into written standard operating procedures to preserve institutional knowledge.

Processes with a one-level gap require structural adjustments. DSS03 and DSS04 need the creation of a centralized knowledge base and a documented, tested disaster recovery plan. MEA02 and MEA03 require the implementation of periodic internal control self-assessments and a formal register to track compliance with data protection regulations.

The two-level gap in DSS05 demands immediate resource allocation. The synod should create a security policy in writing, implement endpoint protection on all management computers, and organize regular vulnerability assessments. If these particular weaknesses are corrected, religious institutions will not only be able to safeguard sensitive information about the congregation but also achieve system continuity while staying clear of corporate IT overhead which is unsustainable.

4. CONCLUSION

This study evaluated the IT governance capability of the SIT GMIM integrated church information system using the COBIT 2019 framework. The evaluation points out that basic operations and monitoring methods are working well. But the dependence here is mostly on informal channels of communication and individual knowledge instead of having written down SOPs. The major governance problems are concentrated on Security management and independent assurance. These areas currently lack formal policies, endpoint protection, and structured evaluation mechanisms.

Theoretically, this research extends the application of COBIT 2019 to the less examined context of religious organizations. It demonstrates that standard capability metrics apply universally, but the root causes of governance gaps in church environments stem from unique structural factors. These factors cover decentralized voluntary activities, limited resources, and a way of life for pastoral people that puts emphasis on being ready to respond over having strict administration. For a practical aspect, this study is of immense help to church IT managers by providing them with the foundation and the improvement roadmap. Religious organizations can reduce operational risk by focusing on low-cost interventions. These interventions include formalizing incident logging, establishing basic disaster recovery documentation, and drafting a foundational information security policy aligned with national data protection laws.

This study has specific limitations. The evaluation is restricted to the central synod management level and covers only the DSS and MEA domains. Future research should expand the assessment to include the EDM, APO, and BAI domains to provide a complete view of enterprise IT governance. Also, studies that come later need also take the point of view of the people at the local level into consideration to know more about how the decisions of the central body influence the delivery of goods and services at the user level. If COBIT 2019 were to be implemented alongside security standards and service management models like ISO/IEC 27001 and ITIL, organizations would get detailed information on how sensitive church members' data should be safeguarded technically.

REFERENCES

[1] GMIM, “SIT GMIM 2.0 | Login.” Accessed: Jul. 22, 2026. [Online]. Available: https://data.gmim.info/login

[2] M. I. Takaendengan *et al.*, "Peningkatan Transparansi Keuangan Gereja Melalui Implementasi Web-Based Church Financial Management System Di Gmim Bukit Zaitun Sea Mitra Minahasa," *ABDI WINA J. Pengabdi. Kpd. Masy.*, vol. 4, no. 2, pp. 51–58, Dec. 2024, doi: 10.58300/abdiwina.v4i2.1000.

[3] Information Systems Audit and Control Association, *COBIT 2019 Framework: Introduction and Methodology*. ISACA, 2018. [Online]. Available: https://books.google.co.id/books?id=PmmDuQEACAAJ

[4] I. P. Windasari, A. F. Rochim, S. N. Alfiani, and A. Kamalia, "Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019," *J Sist. Info Bisnis*, vol. 11, no. 2, pp. 131–138, Jan. 2022, doi: 10.21456/vol11iss2pp131-138.

[5] I. P. Windasari, M. Y. Yonanta, R. Y. Himawati, and A. F. Rochim, "Enterprise Governance of IT Audit Using DSS & MEA COBIT 2019 (Case Study: Faculty of Engineering UNDIP)," *TEKNIK*, vol. 43, no. 1, pp. 67–77, May 2022, doi: 10.14710/teknik.v43i1.34121.

[6] A. Amry, Y. Wirani, and Y. G. Sucahyo, "Assessment of IT Governance Capability Level Using the COBIT 2019 Framework: A Case Study of XYZ Institution," *JEPIN J. Edukasi Dan Penelit. Inform.*, vol. 11, no. 2, pp. 277–286, Aug. 2025, doi: 10.26418/jp.v11i2.95073.

[7] A. Fitri and J. Hartono M, "Evaluasi Penerapan Tata Kelola Teknologi Informasi (TI) Menggunakan Framework Cobit 2019 (Studi Kasus pada Perguruan Tinggi Harapan Maju)," *ABIS Account. Bus. Inf. Syst. J.*, vol. 11, no. 3, p. 225, Sep. 2023, doi: 10.22146/abis.v11i3.86440.

[8] S. D. Putra, H. Herman, and A. Yudhana, "Audit Tata Kelola Academic Information System Menggunakan Framework Cobit 2019," *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 10, no. 3, pp. 467–474, Jul. 2023, doi: 10.25126/jtiik.2023106361.

[9] A. S. Sukamto, H. Novriando, and A. Reynaldi, "Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: UPT TIK Universitas Tanjungpura Pontianak)," *J. Edukasi Dan Penelit. Inform. JEPIN*, vol. 7, no. 2, p. 210, Aug. 2021, doi: 10.26418/jp.v7i2.47859.

[10] H. A. Campbell and G. Evolvi, "Contextualizing current digital religion research on emerging technologies," *Hum. Behav. Emerg. Technol.*, vol. 2, no. 1, pp. 5–17, Jan. 2020, doi: 10.1002/hbe2.149.

[11] P. Purwadi and H. Santoso, "Comparison of Information Technology Governance Maturity Levels Based on COBIT 2019 at PT Kereta Commuter Indonesia in 2023 and 2024," *J. Tek. Inform. Jutif*, vol. 6, no. 5, pp. 2962–2974, Oct. 2025, doi: 10.52436/1.jutif.2025.6.5.5200.

[12] P. Kwak and R. I. Desanti, "IT Governance Evaluation Using COBIT 2019 Framework in A Manufacturing Company," in *2023 7th International Conference on New Media Studies (CONMEDIA)*, Dec. 2023, pp. 62–67. doi: 10.1109/CONMEDIA60526.2023.10428517.

[13] J. Farquhar, N. Michels, and J. Robson, "Triangulation in industrial qualitative case study research: Widening the scope," *Ind. Mark. Manag.*, vol. 87, pp. 160–170, May 2020, doi: 10.1016/j.indmarman.2020.02.001.

[14] IT Governance Institute, *Board Briefing for IT Governance, 2nd Edition*. Information Systems Audit and Control Association, 2003. [Online]. Available: https://books.google.co.id/books?id=MpD2PAAACAAJ

[15] W. Mason *et al.*, "Toward Full Integration of Quantitative and Qualitative Methods in Case Study Research: Insights From Investigating Child Welfare Inequalities," *J. Mix. Methods Res.*, vol. 14, no. 2, pp. 164–183, Apr. 2020, doi: 10.1177/1558689819857972.

[16] M. I. Takaendengan, D. Lapihu, R. Paninggalih, and A. P. Marthinus, "Analyzing the Delivery, Support, and Service (DSS) Domain of UNSRAT Information System using COBIT 5: Identifying Gaps and Opportunities for Improvement," *J. Inf. Technol. Softw. Eng. Comput. Sci. ITSECS*, vol. 1, no. 3, pp. 95–104, Jul. 2023, doi: 10.58602/itsecs.v1i3.51.

[17] M. Destriani and Y. H. Putra, "Rencana Audit Tata Kelola Sistem Informasi Di Universitas Subang Menggunakan Framework COBIT 2019," *J. Tata Kelola Dan Kerangka Kerja Teknol. Inf.*, vol. 9, no. 1, pp. 19–33, May 2023, doi: 10.34010/jtk3ti.v9i1.9164.

[18] M. A. Saputra and M. R. Redo, "Penerapan Framework COBIT 2019 Untuk Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi," *J. Sci. Soc. Res.*, vol. 4, no. 3, p. 352, Oct. 2021, doi: 10.54314/jssr.v4i3.715.

[19] Wahyudi and Sutedi, "Analisis Dan Pengembangan Tata Kelola Teknologi

Informasi Pada Kantor Pos Kotabumi Menggunakan COBIT 2019: Analysis and Development of Information Technology Governance at the Kotabumi Post Office Using COBIT 2019," *JSiI J. Sist. Inf.*, pp. 10–16, Mar. 2025, doi: 10.30656/jsii.v12i1.9771.

[20] G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Perancangan Tata Kelola Teknologi Informasi menggunakan COBIT 2019 pada PT Telekomunikasi Indonesia Regional VI Kalimantan," *J. Sist. Inf. Dan Ilmu Komput. PrimaJUSIKOM PRIMA*, vol. 4, no. 1, pp. 23–30, Sep. 2020, doi: 10.34012/jurnalsisteminformasidanilmukomputer.v4i1.1202.