Designing IT Governance Improvement Priorities Using COBIT 2019 Design Factors: A Case Study of Digital Organizations

Ica Safrila, Muhammad Amin

Abstract

This study aims to design information technology governance improvement priorities using COBIT 2019 Design Factors in digital organizations. The study was conducted using a case study approach with a descriptive-analytical method, integrating quantitative and qualitative data to obtain a comprehensive understanding of the current IT governance condition. Quantitative data were collected through capability level assessment questionnaires based on selected COBIT 2019 governance and management objectives, while qualitative data were obtained through interviews, observation, and document analysis. The COBIT 2019 Design Factors were used to identify organizational context, including enterprise strategy, IT risk profile, threat landscape, compliance requirements, role of IT, sourcing model, technology adoption, and digital service complexity. The results show that most selected COBIT 2019 objectives are positioned at Capability Level 2, indicating that IT governance processes have been implemented and managed but are not yet fully standardized, measured, and continuously improved. The highest capability gaps were found in APO13 – Managed Security, DSS04 – Managed Continuity, APO12 – Managed Risk, and DSS05 – Managed Security Services. These findings indicate that information security governance, IT risk management, service continuity, incident handling, internal control, and compliance monitoring should become the main improvement priorities. This study contributes to the development of a structured, context-based, and evidence-driven IT governance improvement model for digital organizations.

Keywords: *IT Governance; COBIT 2019; Design Factors; Capability Level; Digital Organization; Governance Improvement Priorities*

Ica Safrila[1]
[1]Information Technology, Universitas Pembangunan Panca Budi, Indonesia
e-mail: ichasafrila2709@gmail.com[1]

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

Introduction

Digital transformation has fundamentally reshaped the operational structure of organizations across education, government, and public service sectors. The increasing reliance on information systems has made IT governance a critical component in ensuring that technology investments are aligned with organizational goals, risk management strategies, and service quality expectations [1][2]. In modern digital organizations, IT governance is no longer limited to operational control, but has evolved into a strategic mechanism for value creation and decision support [3].

Empirical studies in Indonesia consistently show that IT governance maturity remains at an intermediate stage. A COBIT 5-based study in a university environment revealed that IT governance processes in the DSS domain were mostly at Capability Level 2 (Managed Process), indicating that operational activities were already running but not yet standardized through formal governance structures [4]. This condition highlights that higher education institutions still face challenges in formalizing IT governance practices despite the availability of established frameworks.

Similar findings are observed in government information systems. A COBIT 2019-based evaluation of SIMPEG (Personnel Management Information System) shows that most DSS processes operate at Level 2, with only partial achievement toward Level 3 [5]. The main gaps identified include lack of standard operating procedures, weak incident management, and limited monitoring mechanisms, which indicate that governance processes are functional but not fully institutionalized.

In addition, studies on Computer-Based Test (CBT) systems in vocational schools demonstrate even lower governance maturity levels, ranging from Level 0 to Level 1 across several COBIT 2019 domains [6]. Critical weaknesses include absence of risk management (APO12), weak security controls (APO13), unstructured solution development (BAI03), and reactive incident handling (DSS02). These findings indicate that without structured governance, digital systems tend to rely heavily on individual operators rather than standardized organizational processes.

Meanwhile, research on digital clipping systems in government institutions using COBIT 2019 shows a relatively more stable governance condition, where APO01, APO11, and APO14 domains consistently achieve Capability Level 2 (Managed Process) with a target of Level 3 [7]. However, despite better operational stability, significant gaps remain in governance formalization, particularly in quality management and data governance structures.

Across these empirical contexts, a consistent pattern emerges: most digital organizations operate at Capability Level 2, indicating that IT processes are executed and monitored but not yet standardized or fully institutionalized. This pattern is consistent with COBIT 2019 capability maturity theory, which states that Level 2 reflects managed but not yet defined processes [8]. The recurring gap lies in the absence of structured governance artifacts such as SOPs, formal policies, and integrated monitoring systems.

From a theoretical perspective, COBIT 2019 introduces a significant advancement through its Design Factors approach, which enables organizations to tailor governance systems based on enterprise strategy, risk profile, and contextual priorities [9]. However, empirical evidence suggests that most organizations still focus on capability assessment rather than using design factors to prioritize governance improvements systematically [10].

This gap is critical because IT governance improvement should not only measure current capability, but also determine prioritized actions that align with organizational context and strategic needs. Without structured prioritization, governance improvements tend to be reactive, fragmented, and inefficient, limiting the overall impact of digital transformation initiatives.

Therefore, this study aims to design IT governance improvement priorities using COBIT 2019 Design Factors in digital organizations. The study synthesizes empirical evidence from multiple contexts, including university IT governance, government SIMPEG systems, CBT examination systems, and digital clipping services, to develop a structured prioritization model. The expected contribution of this research is to bridge the gap between capability assessment and

actionable governance prioritization, enabling organizations to move toward higher levels of IT governance maturity (Level 3 and above).

Research Methodology

2.1 Research Design and Approach

This study employs a case study design with a descriptive-analytical approach to evaluate and establish priorities for improving information technology governance in digital organizations. The case study approach was chosen because it allows for an in-depth analysis of the actual conditions of IT governance implementation within organizational environments characterized by diverse digital features and operational complexities. The primary focus of this study is to identify the gaps between the current state (as-is) and the desired state (to-be) of IT governance, as well as to formulate improvement priorities based on the COBIT 2019 framework.

This research approach integrates quantitative and qualitative methods simultaneously (mixed approach). The quantitative approach is used to measure the level of IT governance process capabilities based on the COBIT 2019 capability model, while the qualitative approach is used to understand the organizational context, process structure, and factors that influence the implementation of IT governance. The combination of these two approaches provides a more comprehensive picture for assessing the state of IT governance both factually and contextually.

The primary framework used in this study is COBIT 2019, specifically the aspects of governance system design and design factors. Design factors are used to tailor governance requirements based on organizational characteristics such as enterprise strategy, risk profile, level of dependence on technology, and the complexity of digital services. The results of the design factors analysis are then mapped to governance and management objectives to identify the priority areas for improving IT governance that are most relevant to the organization's circumstances.

Data collection was conducted using several techniques, including structured questionnaires, interviews with relevant stakeholders, and analysis of organizational documents such as SOPs, IT policies, and system operational reports. The data obtained was then analyzed using the COBIT 2019 capability level calculation method to determine the maturity level of the processes, followed by a gap analysis between the actual conditions and the organization's targets.

The results of this analysis were used to develop a systematic, evidence-based model for prioritizing improvements in IT governance. This model not only illustrates the current level of capability but also provides strategic guidance on which processes should be prioritized for improvement first. Thus, this study is expected to contribute to the development of IT governance that is more adaptive, measurable, and aligned with the needs of modern digital organizations.

The conceptual framework of this study is built upon the COBIT 2019 governance system design, which emphasizes the alignment between enterprise objectives and IT governance implementation through structured design factors. In digital organizations, IT governance is not only assessed based on capability maturity, but also influenced by contextual factors such as organizational strategy, risk profile, technology dependency, and governance priorities. Therefore, COBIT 2019 design factors are used as the primary basis to translate organizational context into governance system design.

This study positions IT governance capability as the dependent construct, which is influenced by the implementation of COBIT 2019 governance and management objectives, particularly across APO, BAI, DSS, and MEA domains. Meanwhile, COBIT 2019 design factors act as the independent contextual variables that determine how governance priorities are structured and which processes require improvement first. The interaction between capability level assessment and design factor analysis forms the basis for determining governance improvement priorities.

The framework integrates three main analytical layers. First, the capability level analysis

measures the current maturity of IT governance processes using the COBIT 2019 capability model (Level 0–5). Second, the gap analysis identifies the difference between current performance (as-is) and expected performance (to-be). Third, the design factors analysis is used to prioritize governance improvement areas based on organizational context. These three layers collectively produce a structured governance improvement model that is both measurable and context-aware.

In this study, governance objectives such as APO12 (Risk Management), APO13 (Security Management), DSS02 (Incident Management), DSS06 (Business Process Control), and MEA03 (Compliance Monitoring) are considered critical indicators of IT governance performance in digital organizations. These objectives are selected based on their relevance to operational stability, data integrity, and service continuity in digital environments.

COBIT 2019 design factors in this study are operationalized into several key dimensions that influence governance prioritization decisions. These include enterprise strategy orientation (growth, innovation, or operational excellence), IT risk profile (low, medium, high), technology adoption level, and dependency on IT systems for service delivery. Each of these factors contributes to determining the weight and priority of governance objectives within the organization.

The integration of design factors with capability assessment results enables the formulation of a governance priority matrix. This matrix maps high-impact governance domains against organizational urgency levels, allowing decision-makers to identify which COBIT processes require immediate improvement and which can be optimized in later phases. This structured prioritization ensures that governance improvements are not implemented uniformly, but instead follow a strategic and risk-informed sequence.

Overall, the conceptual framework of this study follows a structured flow: organizational context is analyzed using COBIT 2019 design factors, IT governance capability is measured through COBIT capability levels, and gaps between current and expected conditions are identified through gap analysis. These results are then synthesized into a prioritized IT governance improvement model that guides organizations in enhancing their digital governance maturity in a structured and evidence-based manner.

The research methodology begins with the identification of organizational context and IT governance conditions within digital organizations. This initial stage involves collecting data related to existing IT governance practices, including operational processes, governance structures, and system performance.

After the organizational context is identified, the study proceeds with the COBIT 2019 Design Factors analysis. This stage evaluates key organizational characteristics such as enterprise strategy, risk profile, IT-related issues, and technology usage level. The purpose of this phase is to determine the most relevant governance and management objectives that should be prioritized.

The next stage involves mapping COBIT 2019 governance objectives into IT governance domains, particularly APO, BAI, DSS, and MEA. Each selected process is then assessed using the COBIT 2019 capability level model to determine the current maturity level (as-is condition).

Following the capability assessment, a gap analysis is conducted by comparing the current capability level with the expected target level (to-be condition). This analysis identifies the differences between actual governance performance and desired organizational standards.

Finally, based on the gap analysis results and design factors prioritization, the study develops an IT governance improvement priority model. This model provides a structured roadmap for organizations to enhance governance maturity in a systematic and evidence-based manner.

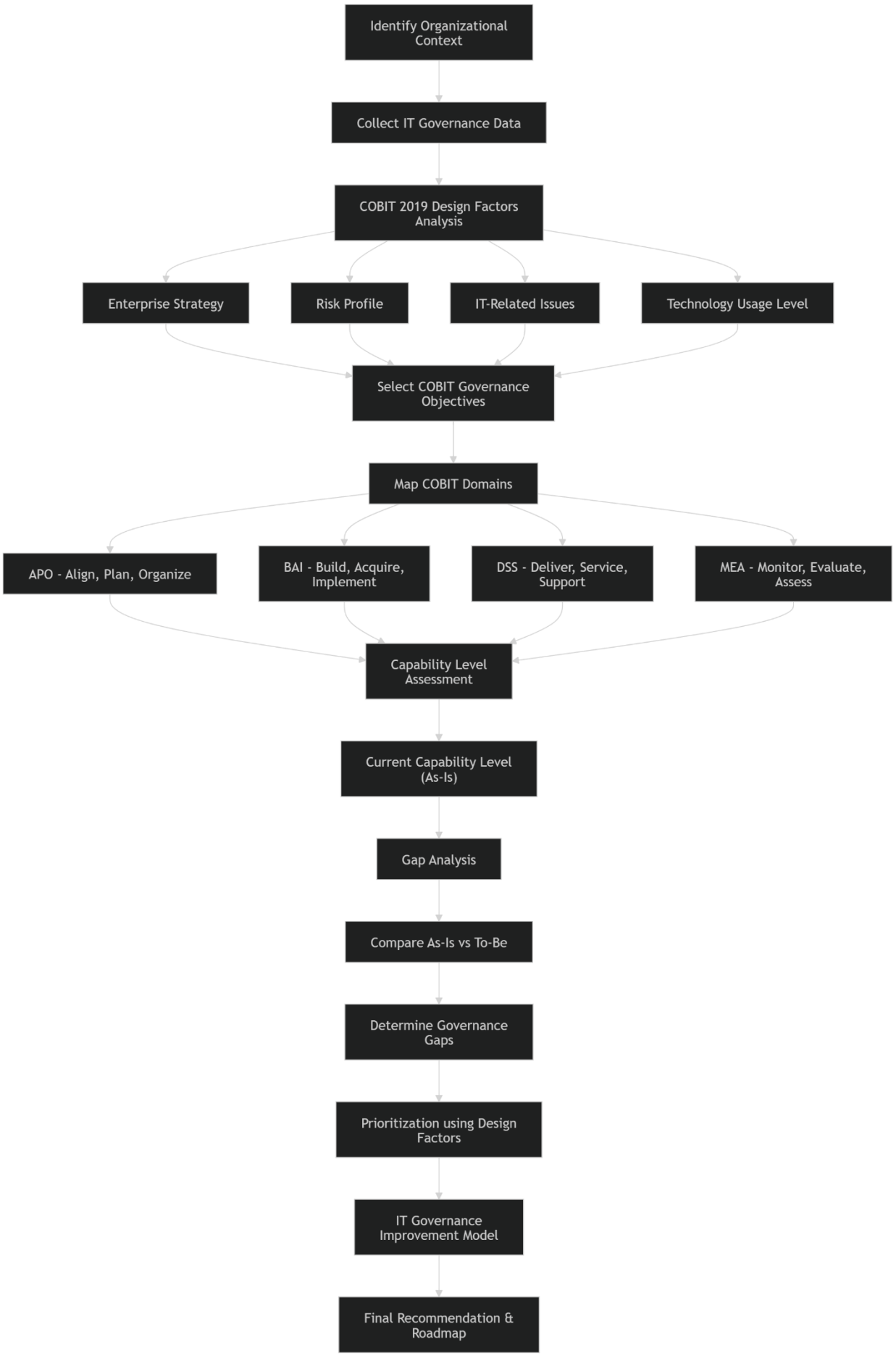

Figure 1. Research Methodology

2.2 Techniques and Sources of Data Collection

Data collection in this study was conducted to obtain comprehensive information regarding the current condition of IT governance, organizational context, digital business characteristics, and factors influencing governance improvement priorities. The data collection techniques were designed based on the COBIT 2019 Design Factors approach, which emphasizes that IT governance should be tailored to the specific context, strategy, risk profile, regulatory environment, technology adoption, and role of IT within an organization. COBIT 2019 recognizes that there is no single governance design suitable for all organizations; therefore, each organization needs to identify its own design factors to determine the most relevant governance and management objectives.

2.3 Research Instrument

The research instrument in this study was developed to collect data related to the organizational context, IT governance condition, and COBIT 2019 Design Factors. The instrument was designed to support the identification of IT governance improvement priorities in digital organizations. COBIT 2019 emphasizes that governance and management objectives should be tailored to the specific characteristics of each organization through design factors, because there is no single governance system that fits all organizations. These design factors include enterprise strategy, enterprise goals, risk profile, IT-related issues, threat landscape, compliance requirements, role of IT, sourcing model, implementation methods, technology adoption strategy, and enterprise size.

2.4 Quantitative Data Analysis Techniques

The quantitative data in this study were analyzed to determine IT governance improvement priorities based on COBIT 2019 Design Factors. COBIT 2019 emphasizes that governance systems should be tailored to organizational characteristics because there is no single governance model that fits all enterprises. The design factors are used to describe organizational context, strategy, risk exposure, compliance requirements, role of IT, sourcing model, implementation method, technology adoption, and enterprise size. Quantitative analysis was conducted through several stages: data coding, descriptive statistical analysis, validity and reliability testing, design factor scoring, capability gap analysis, and priority ranking of COBIT 2019 governance and management objectives.

2.5 Qualitative Data Analysis Techniques

Qualitative data analysis in this study was conducted to interpret data obtained from interviews, observations, and document reviews. The purpose of qualitative analysis was to obtain a deeper understanding of the organizational context, IT governance practices, IT-related issues, risk exposure, compliance needs, and factors influencing IT governance improvement priorities. The qualitative findings were used to complement the quantitative results and explain why certain COBIT 2019 governance and management objectives became priority areas for improvement. The qualitative analysis was carried out through several stages, including data transcription, data reduction, coding, categorization, theme development, triangulation, and conclusion drawing.

Results

3.1 Characteristics of Research Respondents

The respondents in this study were selected based on their involvement, knowledge, and responsibility in IT governance, digital transformation, risk management, information security, IT operations, and business process management within the digital organization. Since the study aimed to design IT governance improvement priorities using COBIT 2019 Design Factors, the respondents were required to have sufficient understanding of the organization's IT strategy, governance practices, IT risks, technology adoption, compliance requirements, and operational challenges.

The selection of respondents was conducted using a purposive sampling technique. This technique was considered appropriate because the study required information from individuals who were directly involved in IT governance processes and who could provide relevant data regarding the current condition of IT governance in the organization.

Table 1. Respondent Selection Criteria

No.	Criteria	Description
1	Involvement in IT governance	Respondents are involved in IT decision-making, IT planning, IT risk management, or IT service management.
2	Knowledge of organizational strategy	Respondents understand the organization's digital strategy, business objectives, and IT contribution to business performance.
3	Experience with IT processes	Respondents have experience in managing, using, auditing, or evaluating IT systems and digital services.
4	Relevance to COBIT 2019 Design Factors	Respondents can provide information related to enterprise strategy, enterprise goals, IT risk profile, IT-related issues, threat landscape, compliance requirements, role of IT, sourcing model, implementation methods, technology adoption, and enterprise size.
5	Minimum work experience	Respondents have worked in the organization or related IT function for at least one year, so they understand the organization's IT governance practices.

3.2 COBIT 2019 Capability Level Measurement Results

The capability level measurement was conducted to determine the current condition of IT governance practices in the digital organization. The assessment focused on selected COBIT 2019 governance and management objectives that were considered relevant based on the analysis of COBIT 2019 Design Factors.

COBIT 2019 consists of governance and management objectives grouped into five domains, namely EDM, APO, BAI, DSS, and MEA. The EDM domain focuses on governance activities, while APO, BAI, DSS, and MEA focus on management activities related to planning, implementation, service delivery, monitoring, and evaluation. COBIT 2019 also supports a CMMI-based process capability scheme, where the capability level ranges from 0 to 5 and reflects how well a process is implemented and performing.

Table 2. Capability Level Measurement Scale

Capability Level	Interpretation	Description
0	Incomplete	The process is not implemented or does not achieve its purpose.
1	Performed	The process is implemented but still informal and inconsistent.
2	Managed	The process is planned, monitored, and partially controlled.
3	Established	The process is defined, standardized, and documented.
4	Predictable	The process is measured, controlled, and consistently implemented.
5	Optimizing	The process is continuously improved based on performance evaluation.

In this study, the current capability level represents the actual condition of the organization, while the target capability level represents the expected condition based on organizational needs, digital business characteristics, and COBIT 2019 Design Factor analysis.

Table 3. COBIT 2019 Capability Level Measurement Results

No.	COBIT 2019 Objective	Domain	Current Capability Level	Target Capability Level	Gap	Priority Status
1	EDM03 – Ensured Risk Optimization	EDM	2.20	4.00	1.80	High
2	APO12 – Managed Risk	APO	2.10	4.00	1.90	Very High
3	APO13 – Managed Security	APO	2.00	4.00	2.00	Very High
4	APO14 – Managed Data	APO	2.30	4.00	1.70	High
5	APO10 – Managed Vendors	APO	2.40	3.00	0.60	Moderate
6	BAI02 – Managed Requirements Definition	BAI	2.30	3.00	0.70	Moderate
7	BAI03 – Managed Solutions Identification and Build	BAI	2.50	3.00	0.50	Moderate
8	BAI06 – Managed IT Changes	BAI	2.20	4.00	1.80	High
9	BAI11 – Managed Projects	BAI	2.10	3.00	0.90	Moderate
10	DSS01 – Managed Operations	DSS	2.50	4.00	1.50	High
11	DSS02 – Managed Service Requests and Incidents	DSS	2.20	4.00	1.80	High
12	DSS04 – Managed Continuity	DSS	2.00	4.00	2.00	Very High
13	DSS05 – Managed Security Services	DSS	2.10	4.00	1.90	Very High
14	MEA01 – Managed Performance and Conformance Monitoring	MEA	2.30	4.00	1.70	High
15	MEA02 – Managed System of Internal Control	MEA	2.20	4.00	1.80	High
16	MEA03 – Managed Compliance with External Requirements	MEA	2.40	4.00	1.60	High

Table 4. Summary of Capability Level by Domain

COBIT 2019 Domain	Number of Objectives Assessed	Average Current Capability	Average Target Capability	Average Gap	Interpretation
EDM	1	2.20	4.00	1.80	Risk governance needs improvement
APO	4	2.20	3.75	1.55	Planning, risk, security, and data governance need strengthening
BAI	4	2.28	3.25	0.98	IT project and change management are moderately developed
DSS	4	2.20	4.00	1.80	IT service delivery, continuity, and security services require improvement

COBIT 2019 Domain	Number of Objectives Assessed	Average Current Capability	Average Target Capability	Average Gap	Interpretation
MEA	3	2.30	4.00	1.70	Monitoring, internal control, and compliance need strengthening

Based on the domain-level analysis, the lowest average current capability was found in the APO and DSS domains, with an average score of 2.20. This indicates that the organization has implemented planning, risk management, security management, service delivery, and operational support processes, but these processes have not yet reached a standardized and measurable level.

3.3 Results Capability Gaps

Table 5. Highest Capability Gaps

Rank	COBIT 2019 Objective	Current Level	Target Level	Gap	Interpretation
1	APO13 – Managed Security	2.00	4.00	2.00	Information security governance requires urgent improvement.
2	DSS04 – Managed Continuity	2.00	4.00	2.00	IT continuity planning and disaster recovery need to be strengthened.
3	APO12 – Managed Risk	2.10	4.00	1.90	IT risk management is not yet fully integrated and measurable.
4	DSS05 – Managed Security Services	2.10	4.00	1.90	Operational security controls need more consistent implementation.
5	EDM03 – Ensured Risk Optimization	2.20	4.00	1.80	Governance-level risk oversight needs improvement.
6	BAI06 – Managed IT Changes	2.20	4.00	1.80	IT change management needs stronger control and documentation.
7	DSS02 – Managed Service Requests and Incidents	2.20	4.00	1.80	Incident management requires faster response, escalation, and monitoring.
8	MEA02 – Managed System of Internal Control	2.20	4.00	1.80	Internal control monitoring needs to be improved.

The capability level measurement results indicate that the digital organization has already implemented several IT governance and management practices. However, most of the assessed objectives are still at Level 2, meaning that the processes are already managed but have not yet been fully standardized, measured, and optimized.

The highest capability gaps were found in APO13 – Managed Security, DSS04 – Managed Continuity, APO12 – Managed Risk, and DSS05 – Managed Security Services. These findings indicate that the organization needs to prioritize improvements in information security governance, IT continuity management, risk management, and operational security services. This result is consistent with the characteristics of digital organizations, where business processes are highly dependent on information systems, digital platforms, data availability, and cybersecurity protection.

3.4 Discussion

The results of the COBIT 2019 capability level measurement indicate that the digital

organization has implemented several IT governance and management practices, but most of them remain at a managed level rather than a standardized, measurable, and continuously improved level. This condition shows that the organization already recognizes the importance of IT governance; however, the implementation is still not fully mature. In practical terms, several IT processes are already performed and monitored, but the consistency of documentation, performance measurement, control evaluation, and continuous improvement still requires further strengthening.

The dominance of capability level 2 across several COBIT 2019 objectives suggests that the organization has moved beyond informal IT management practices but has not yet achieved a fully established governance system. This finding is important because digital organizations are highly dependent on information systems, digital platforms, data availability, cybersecurity, and reliable IT services. In this context, IT is not merely a supporting function but a strategic component that directly affects service delivery, operational continuity, customer experience, and organizational competitiveness. Therefore, IT governance improvement should not only focus on technical problem solving but also on strengthening strategic alignment, risk-based decision-making, and governance accountability.

The use of COBIT 2019 Design Factors in this study provides a context-based approach to determining governance improvement priorities. COBIT 2019 emphasizes that governance systems should be tailored to the specific characteristics of each organization, including enterprise strategy, enterprise goals, risk profile, threat landscape, compliance requirements, role of IT, sourcing model, implementation methods, technology adoption strategy, and enterprise size. This means that IT governance improvement cannot be designed using a one-size-fits-all approach. Each organization needs to identify which governance objectives are most relevant to its business context and digital transformation needs.

The highest capability gaps were found in objectives related to information security, IT risk management, service continuity, and security services. This finding reflects the characteristics of digital organizations that are increasingly exposed to cybersecurity threats, operational disruptions, data protection issues, and compliance pressure. Objectives such as APO13 – Managed Security, APO12 – Managed Risk, DSS04 – Managed Continuity, and DSS05 – Managed Security Services therefore become critical areas for improvement. Weaknesses in these areas may increase the possibility of cyber incidents, data breaches, system downtime, and loss of stakeholder trust.

The high gap in APO13 – Managed Security indicates that information security governance needs to be improved at the planning and organizational level. Security should not only be treated as a technical responsibility of the IT department but also as an organizational governance issue. This includes defining security policies, assigning clear roles and responsibilities, establishing security risk assessments, increasing user awareness, and ensuring that security controls are aligned with organizational risks. In digital organizations, weak security governance can directly affect business continuity and public trust, especially when digital services process sensitive or high-value data.

The high gap in DSS04 – Managed Continuity also shows that the organization needs stronger continuity planning and disaster recovery management. Digital organizations depend heavily on system availability; therefore, service interruption can have serious consequences for operational performance. The organization needs to ensure that business continuity plans, backup mechanisms, disaster recovery procedures, recovery time objectives, and incident response mechanisms are clearly defined, documented, tested, and improved periodically. This finding strengthens the argument that IT continuity management should be treated as one of the main priorities in governance improvement.

The results also show that APO12 – Managed Risk and EDM03 – Ensured Risk Optimization require significant attention. This indicates that IT risk management has not been fully integrated into governance-level decision-making. Risk identification, risk assessment, mitigation planning, and monitoring should be connected to strategic objectives and digital transformation initiatives. COBIT 2019 supports the use of governance and management

objectives to help organizations evaluate, direct, and monitor IT-related risks so that information and technology can deliver value while remaining within acceptable risk levels.

Conclusion

This study concludes that the use of COBIT 2019 Design Factors provides a structured and context-based approach for determining IT governance improvement priorities in digital organizations. The capability level measurement shows that most selected governance and management objectives are still at the managed level, indicating that IT governance practices have been implemented but are not yet fully standardized, measured, and continuously improved. The main improvement priorities are found in the areas of information security, IT risk management, service continuity, incident management, internal control, and compliance monitoring. These priorities reflect the characteristics of digital organizations that depend heavily on reliable information systems, data protection, cybersecurity, and uninterrupted digital services. Therefore, the proposed IT governance improvement should focus on strengthening critical COBIT 2019 objectives such as APO13, APO12, DSS04, DSS05, EDM03, DSS02, MEA02, and MEA03. By prioritizing these areas, the organization can improve its governance capability, reduce IT-related risks, enhance service reliability, and ensure that information and technology better support organizational goals and digital transformation.

References

[1] W. Van Grembergen and S. De Haes, *Enterprise governance of information technology: Achieving strategic alignment and value*. 2009. doi: 10.1007/978-0-387-84882-2.

[2] I. Yuhertiana, G. A. Husna, and E. Susilowati, "Audit Committee and ESG Disclosure: Advancing SDG for Sustainable Performance in State-Owned Enterprises," *J. Lifestyle SDGs Rev.*, vol. 5, no. 1, 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n01.pe05042.

[3] J. Schneider, R. Abraham, C. Meske, and J. Vom Brocke, "Artificial Intelligence Governance For Businesses," *Inf. Syst. Manag.*, vol. 40, no. 3, 2023, doi: 10.1080/10580530.2022.2085825.

[4] H. R. Septian *et al.*, "Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus : Universitas Pembangunan Panca Budi Medan)," *Audit Tata Kelola Teknol. Inf. menggunakan Cobit 5 (Studi Kasus Univ. Pembang. Panca Budi Medan)*, vol. 6, 2019.

[5] A. G. Nainggolan and R. F. Wijaya, "Capability Analysis in IT Governance for Enhancing SIMPEG Services Using the DSS Domain of COBIT 2019," pp. 7793–7803, 2019.

[6] "Implementation of COBIT 2019 Framework in Governance of Computer- Based Test (CBT) Examination System at SMK Muhammadiyah 10 Kisaran," pp. 7699–7704, 2019.

[7] A. P. U. Siahaan, E. P. B. Barus, M. Hasanuddin, Zulfan, and F. Rizaldi, "Perancangan Peningkatan Tata Kelola Ti Kliping Digital di Instansi Pemerintahan Menggunakan Pendekatan Manajemen Informasi," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 3, 2026, doi: 10.62712/juktisi.v4i3.762.

[8] S. Dewangga and B. Trias Hanggara, "Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. Kreatiful Digital Indonesia menggunakan Framework COBIT 2019," *... Teknol. Inf. dan ...*, vol. 7, no. 5, pp. 2597–2606, 2023, [Online]. Available: http://j-ptiik.ub.ac.id

[9] D. Darmawan and A. F. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," *J. Comput. Inf. Syst. Ampera*, vol. 3, no. 1, 2022, doi: 10.51519/journalcisa.v3i1.139.

[10] O. Turel and C. Bart, "Board-level IT governance and organizational performance," *Eur. J. Inf. Syst.*, vol. 23, no. 2, pp. 223–239, 2014, doi: 10.1057/ejis.2012.61.