Core model of information technology governance system design in local government

Lanto Ningrayati Amali, Muhammad Rifai Katili, Sitti Suhada
Department of Informatics Engineering, Faculty of Engineering, Universitas Negeri Gorontalo, Gorontalo, Indonesia

Article Info

ABSTRACT

Information technology governance (ITG) in local government is aimed at a good governance service framework. Reports produced as a result of the framework's implementation help to improve governance's openness, potency, and efficiency. A strong governance structure for adopting information technology (IT) is essential to ensuring its best utilization. The governance system should be properly managed to support the organization's business. Therefore, this research aims to design an ITG system suitable for best practices using the control objectives for information technologies (COBIT) 2019 framework. The recommendations from the core model were processed based on the priority or competence level that local government entities use. It also produced a core model with capability levels of 1 and 2 that do not exist. The recommendation designated for the priority level of 3 was 17. The core model to be assigned a capability level of 4 urgently needed to be implemented was 23 core models.

Corresponding Author:

Muhammad Rifai Katili
Department of Informatics Engineering, Faculty of Engineering, Universitas Negeri Gorontalo
Prof. Dr. Ing. B. J. Habibie Street, Gorontalo, Indonesia
Email: mrifaikatili@ung.ac.id

1. INTRODUCTION

Advances in information technology (IT) platforms have introduced an increasingly complex layer in the planning and decision-making processes [1]-[3], as well as support organizations in the delivery of goods and services to customers. Nearly all company activities involve IT, which is seen as a strategic opportunity to gain an advantage over competitors [4]. Its use in many organizations has made information technology governance (ITG) highly regarded since its inception in the early 1990s [5]-[7]. Interest in the role and relevance of IT has increased. Therefore, the proper management of these conditions is necessary. Applying the Indonesian Government System regulated by Presidential Instruction No. 3 of 2003 highlights the need to use information and communications technology (ICT) for government purposes. The application, both at the central and regional levels, requires professional management, human resources, high costs, and risk of failure. Therefore, an understanding of the use, development, and guidelines governing the utilization of organizational IT and the practice of an effective decision-making model is required [8].

IT is an integral part of most establishments and promises to become more integrated into the organization [9]–[11]. Considering the implementation of the ITG in Indonesia, this program has faced many challenges, both from the Council of Authorities and other bureaucratic institutions. The cause of these problems was 80% due to non-ICT elements (bureaucracy, politics, human resources, and power) and 20% related to ICT factors (system quality and reliability) [12]. The need for organized ITG is driven by the demand for clean, transparent administration, risk protection, costs, and opportunities related to implementation.

The public sector demands the ITG achieve its vision, mission, and goal. This is not always feasible because it causes problems that hinder public service performance [13]. As an organizational capability, ITG is critical for strategic alignment and business delivery. Unfortunately, the outcomes and contributions of ITG are poorly understood [14], [15]. This is because executive or organizational leadership has not yet acquired the knowledge to develop their business through technology. Although it is supported by sophisticated software running on reliable hardware, optimal implementation is impossible without appropriate management. Designing and understanding good governance should avoid implementation failures, adopt IT recovery during disasters, and sustain operations under every condition. This aligns with research that states that understanding the concept of governance is important because it sets the boundaries and scope of function and government purpose [16].

The directors' board and executive management are in charge of ITG. Thus, it should be a crucial component of the overall administration, which consists of the organizational structure and leadership of current processes, to maintain the continuity of the established IT and create strategies and objectives [17]. Another concept states that the government applies ideas borrowed from organizational administration to strategically direct and control IT, specifically related to two main issues: the value technology provides to establishments and the control and mitigation of the related risks [18], [19]. This shows that IT has shifted from technology to management. Hence, they should be managed as other organizational assets. The implementation should be carried out correctly and supported by good governance from the planning to the application stage.

Effective ITG is built on several essential pillars: leadership, organization, proper decisions, flexibility, scalable processes, and available technology [20], [21]. Organizations must use well-designed, understood, transparent mechanisms [21], [22]. However, good governance arrangements are expected to fail when the supporting tools are not implemented adequately. To facilitate its implementation, a study was conducted on the mechanisms, procedures, and structures of the ITG. Implementing this governance is very important for organizations to generate tangible business benefits such as good reputation, trustworthiness, and reduced costs [23]. Moreover, it aims to enhance and ensure the effective use of resources as an essential factor for organizational success [24]. According to some studies, the aim is to ensure value creation from investments and reduce IT-related risks [25], [26]. Therefore, effective governance is necessary and not an option [27], [28].

ITG is one of the crucial instruments used by managers presently, as it is no longer only a support but also a strategic tool that drives the business. Organizations need to understand the process of managing IT in a dynamic and competitive world rather than only using it. Additionally, governance is concerned with assigning responsibilities and making the right decisions to drive desired behavior, generate value from IT investments, and fully align with the organization's business strategy and direction [29]. This impacts the organization's overall performance, but there are still difficulties in understanding the influencing factors [30]. Design factors influence organizational systems and position them for successful use [31]. It is essential to consider several governance and management goals if IT is to help accomplish organizational goals significantly. As a reference tool, control objectives for information technologies (COBIT) 2019 has established a core model with governance and management goals. This is important for understanding the problems and strategic benefits of IT, ensuring the effectiveness of governance, and facilitating implementation adapted to business conditions.

2. METHOD

The method aimed to clarify what to achieve in research, and problem-solving can run following attaining the objectives. Therefore, a quantitative technique was used to collect data from the 15 respondents through questionnaires. Observations, documentation, and interviews with several stakeholders were conducted to strengthen the questionnaires. This research was conducted at the Information and Statistics Communications and Statistics Office of Gorontalo Province, which has developed e-government and IT activities. Interviews were held with the directors of infrastructure, application development, and e-government. The data analyses used the input values for the 11 design factors in the COBIT 2019 design tool kit.

Design factors can affect an organization's governance structure, placing it in a successful I&T position. The goal cascade of an organization is one of the stages of the design factors, as depicted in Figure 1. From the figure, the core model of the governance system is limited to variant components, including the threat landscape, compliance requirements, IT role, and enterprise size. This approach will result in suggestions for management objectives and ranking governance or related governance system components, establishing target capacity levels, or implementing certain governance system component modifications.

There are two types of components of the 2019 COBIT governance system consist of 2 types: generic and variant in the core model and the application of its principles. Although it is based on a generic component, this variant has been altered for a particular purpose or set in a specific area of emphasis. This research focused on information security, DevOps, and the fulfilment of specific regulations as the strategic alignment of IT and

the delivery of the organization's business in line with the limited core model components. Furthermore, the assessment of design factors includes four stages, as shown in Figure 2 with the explanation. The various steps and processes in the design process, as depicted in Figure 2, will result in recommendations for ranking governance and management goals or related setting target capability levels, governance system components, or implementing particular variations of a governance system component.

Figure 1. COBIT design factors

Figure 2. Governance system design workflow

3. RESULTS AND DISCUSSION

The workflow of the four governance systems is explained in terms of the design stages depicted in Figure 2. Firms should customize their governance systems by considering design factors to maximize the benefits of using technology. A set of design elements must be used as guidelines for changing and prioritizing the constituent parts of the governance system to create an effective governance system for the company.

3.1. Understanding the organizational context and strategy

Understanding organizational strategy helps to identify the most appropriate method based on archetypes. Organizations usually have one primary or secondary archetype or pattern. For example, other value design factors become secondary archetypes when the primary system is innovative/differentiated. There are four archetypes: growth/acquisition, which focuses on development and profit; innovation/differentiation; providing innovative services or products; cost leadership; minimizing short-term costs; client service/stability-enhancing stability; and user-oriented services [31].

Understanding organizational aims as a strategy can be realized by achieving these goals. There are 13 goals with the organization's ability to distinguish between primary and secondary types, broken down into four perspectives: customer, financial, growth, and internal. Analyzing IT-related risks is necessary at the stage of understanding the profile. Nineteen risk profiles were identified, and the findings of previous studies turned into goals for governance and management. The next step involved understanding IT concerns, where 20 currently connected risks or difficulties were discovered by examining the organization's audit records, management reports, or interviews [31].

3.2. Determining the governance system's initial scope

The stage establishes the governance system's initial scope by leveraging information from earlier studies. Figure 3 shows the organizational strategy. The value of client service/stability is five in the primary process. The organization focuses on providing services to the community, and the overall implementation of the ITG is fulfilled.

Figure 4 illustrates the financial worth of organizational goals. The main goal, EG03-compliance with external rules and regulations, has a value of 5. This is because the organization always complies with existing rules and regulations. Besides, the establishment is in a heavily regulated field with a significant risk when they do not abide by the rules and regulations of the government. From the viewpoint of the customer, EG05-customer-oriented service culture-and EG06-business-service continuity and availability-are important objectives worth 5 points each. This is because organizations provide maximum service quality to the community, support public activities, and implement government proceedings.

The value of organizational goals in the perspective of internal EG09-optimization of business process costs, including EG10-staff skills, motivation, and productivity, as well as the EG11-compliance with internal policies are assigned primary goals with a value of 5. The organization remains focused on optimization and cost efficiency without reducing the quality of public services. Therefore, to provide good public services, the organization focuses on human resources with the ability, skills, and work motivation and all organizational policies with the government.

The value for organizational goals from a growth perspective EG12-managed digital transformation programs and EG13 product and business innovation is 5. Organizations attempt to be more responsive to changes and environmental demands. To improve benefits, such as cost savings, efficiency gains, and service effectiveness, innovation must be continued through the development, design, and use of digital technology for company activities and processes. Thus, regardless of size, all organizations and industries may run more effectively and provide value to their customers.

In Table 1, the main priority in this risk profile, with an impact value of 5, is IT operational infrastructure incidents, with a rating of 10. This is because errors/damages sometimes occur but should be repaired quickly to provide good service to the community, this rarely occurs. Therefore, the likelihood was 2. Hardware incidents have a risk rating of 10 because their impact on business processes in the form of public services is enormous, such as servers experiencing interference.

Meanwhile, logical attacks (hacking and malware) have a risk rating of 25 because they significantly impact the organization's information assets and data security. Third-party/supplier incidents have a risk rating of 10 because the organization uses IT services from Internet providers. When damage or disruption occurs to the provider, it affects public services; that is, the impact of this risk scenario is five, and the likelihood is two.
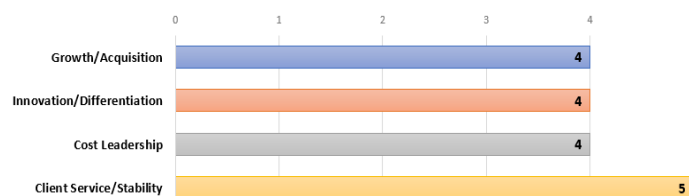

Figure 3. Design factors enterprise strategy

Figure 4. Design factors enterprise goals

Table 1. Design factor IT risk profile

Risk scenario category	Impact (1–5)	Likelihood (1–5)	Risk rating	Baseline
IT investment decision-making, portfolio definition and maintenance	4	2	8	9
Program and projects life cycle management	4	3	12	9
IT costs and oversight	3	2	6	9
IT expertise, skills and behavior	3	4	12	9
Enterprise/IT architecture	3	2	6	9
IT operational infrastructure incidents	5	2	10	9
Unauthorized actions	4	4	16	9
Software adoption/usage problems	4	3	12	9
Hardware incidents	5	2	10	9
Software failures	4	3	12	9
Logical attacks (hacking and malware)	5	5	25	9
Third-party/supplier incidents	5	2	10	9
Noncompliance	3	3	9	9
Geopolitical issues	1	2	2	9
Industrial action	3	3	9	9
Acts of nature	3	3	9	9
Technology-based innovation	3	3	9	9
Environmental	3	3	9	9
Data and information management	4	4	16	9

For the challenges of information technology, the results of the previous understanding were translated into priorities for governance and management purposes. This shows that among the 20 IT-related issues, as shown in Figure 5, some have an interest of 1, indicating no problem. Moreover, some have an interest of 2, which is problematic, and an interest of 3, which is a serious issue. Considering the organization's risk profile and the present I&T-related challenges, the company must know these results. If these technical issues are not addressed, they can hinder worker productivity, jeopardize the security of sensitive data, and compromise company processes.

3.3. Determining the governance system's initial scope

The threat environment in which the organization operates (Table 2) is:

a)   Organizations have an IT threat landscape of 10% high because comprehensive data protection and information security in digitalization are overcome by issuing regulations related to implementing information security within government agencies. The regulations issued were in the form of laws and decrees by the Minister of Communication and Information Technology.

b)   Organizations have an IT threat landscape of 10% normal because of the use of increasingly complex. IT causes vulnerabilities and menaces, including confidentiality, integrity, and service availability, which can disrupt the performance of public service providers.

Table 2. Design factor threat landscape

Value	Importance (100%)	Baseline
High	10%	33%
Normal	10%	67%

The compliance requirements that are the targets of the organization (Table 3) are:

a)   The organization has 100% high compliance requirements because it should obey and comply with regulations where all activities are appropriate with applicable policies, rules, regulations, and laws.

b)   The organization has 100% normal compliance requirements because the wheels of the establishment run appropriately with the vision and mission that has been declared. It is subjected to a series of standard compliance requirements for local government establishments.

c)   The organization has 40% low compliance requirements because they do not need many prerequisites. Therefore, compliance needs were very high.

Table 3. Requirements for design factor compliance

Value	Importance (100%)	Baseline
High	100%	0%
Normal	100%	100%
Low	40%	0%

According to Table 4, an organization's use of IT includes:

a) IT plays a significant role in the Gorontalo provincial government. Therefore, the support value was 5. Some information system/information technology (IS/IT) also supports organizations' business processes.

b) The factory is worth one because the organization's business processes and services still run despite IT failures.

c) The turnaround is worth five because IS/IT is very supportive of the automation of business processes and organizational services needed by the community.

d) Strategic value is 5. Providing excellent public services is the goal of all local governments. Therefore, IS/IT is critical for business processes and services. IS/IT simplifies the service process, introduces regional potential, and increases interactions between the community and business.

Figure 5. Design factors IT-related issues

Table 4. IT's role as a design factor

Value	Importance (1–5)	Baseline
Support	5	3
Factory	1	3
Turnaround	5	3
Strategic	5	3

The adopted organizational resource model for IT (Table 5) is described:
a) The value of the outsourcing model is 20% because organizations still need resources to develop or produce service products that tend to be complicated. Some services are standardized using products provided by the government.
b) The cloud model is worth 30% because several IS/IT services use cloud systems in business processes and services.
c) Using 100% in-source or existing resources with a workforce in IS/IT aligns with the organization's needs to create their IS/IT by utilizing open-source system development.

Table 5. Model for IT design factor sourcing

Value	Importance (100%)	Baseline
Outsourcing	20%	33%
Cloud	30%	33%
Insourced	100%	34%

Organizations adopt IT implementation methods (Table 6) described:
a) The value of agile methods is 100% because IS/IT in an organization is crucial for supporting business processes and public services, indicating that its development is implemented before the service is released.
b) DevOps implementation is worth 80% because experts support human resources in IS/IT. Hence, the service quality is maintained.
c) Implementing the traditional method is worth 80% because some services have a high level of complexity. Hence, this method is suitable for simplifying the design and management of requirements.

Table 6. Design factor IT implementation method

Value	Importance (100%)	Baseline
Agile	100%	15%
DevOps	80%	10%
Traditional	80%	75%

Table 7 presents the technology adoption strategy with the description.
a) Organizations have a first-mover value of 100%, where they should be able to adapt to IS/IT developments better in providing good services to the public; hence, organizations generally adopt new technologies.
b) Followers are worth 80% because the organization has resources capable of implementing IS/IT development.
c) The slow adopter value is 60% because not all existing human resources adapt directly to IS/IT changes. Therefore, training is required for most human resources.

Table 7. Design factor technology adoption strategy

Value	Importance (100%)	Baseline
First mover	100%	15%
Follower	80%	70%
Slow adopter	60%	15%

The size of the enterprise related to the design of the organizational governance system is described as: the organization has more than 250 full-time employees and is a large organization. Because of their enormous budgets, these organizations can afford to be more nimble when spending on technology.

Therefore, IS/IT is designed to address all potential organizational problems related to public services. These types of solutions require considerable expertise for implementation. The IT Infrastructure of this organization is partly built using ready-to-use consumer technology. Organizations also need a centrally managed and monitored IT solution for all user security and bandwidth requirements.

3.3.1. Conclude the governance system

Based on the design factor mapping, the results of the ITG system are obtained, as shown in Figure 6 and explained in Table 8. This indicates that organizations should consider design governance and management objectives to build the most suitable and adaptable governance system. Besides that, it helps management understand the IT governance system, as well as helps management decide on the necessary controls.

The technology management system is a core process model with recommended priority and capability levels. Governance/management goals that score or have a priority of 75 or higher require an ability level of four. Those prioritizing 50 or more required a capability level of 3. A score of 25 or higher indicates an ability level of 2. Meanwhile, for governance/management objectives with a score of less than 25, the process should reach a capability level of 1.

Table 8 shows that the no-core model has capability levels 1 and 2. Therefore, 17 and 23 core models are recommended to have a priority of 3 and 4, respectively. Considering these results, organizations must consider a core model with Level 4 capabilities, as shown in Table 9.

Table 8. ITG and management design summary

Core model	Priority	Capability level suggestion
EDM01 - ensured governance framework setting and maintenance	65	3
EDM02 - ensured benefits delivery	65	3
EDM03 - ensured risk optimization	75	4
EDM04 - ensured resource optimization	60	3
EDM05 - ensured stakeholder engagement	75	4
APO01 - managed IT management framework	75	4
APO02 - managed strategy	65	3
APO03 - managed enterprise architecture	80	4
APO04 - managed innovation	60	3
APO05 - managed portfolio	65	3
APO06 - managed budget and costs	50	3
APO07 - managed human resources	80	4
APO08 - managed relationships	75	4
APO09 - managed service agreements	60	3
APO10 - managed vendors	70	3
APO11 - managed quality	65	3
APO12 - managed risk	85	4
APO13 - managed security	85	4
APO14 - managed data	70	3
BAI01 - managed programs	75	4
BAI02 - managed requirements definition	90	4
BAI03 - managed solutions identification and build	100	4
BAI04 - managed availability and capacity	65	3
BAI05 - managed organizational change	80	4
BAI06 - managed IT changes	90	4
BAI07 - managed IT change acceptance and transitioning	90	4
BAI08 - managed knowledge	70	3
BAI09 - managed assets	65	3
BAI10 - managed configuration	90	4
BAI11 - managed projects	80	4
DSS01 - managed operations	75	4
DSS02 - managed service requests and incidents	75	4
DSS03 - managed problems	75	4
DSS04 - managed continuity	80	4
DSS05 - managed security services	90	4
DSS06 - managed business process controls	70	3
MEA01 - managed performance and conformance monitoring	70	3
MEA02 - managed system of internal control	65	3
MEA03 - managed compliance with external requirements	80	4
MEA04 - managed assurance	75	4

Table 9. Core models recommendation

| Reference	Recommended
EDM03 - ensured risk optimization	Ensure that IT-related risks do not exceed the tolerance. The possibility for compliance failures must be reduced, and the risk impact on corporate value must be evaluated and controlled.
EDM05 - ensured stakeholder engagement	a) To increase performance, ensure stakeholders support the IT strategy and roadmap, establish reporting bases, and promote effective and timely communication. b) Identify areas for development and ensure that organizational strategy and IT-related goals are compatible.
APO01 - managed IT management framework	To address the organization's governance needs, adopt a consistent management strategy. This encompasses organizational structure, roles and duties, consistent and repeatable operations, information items, rules and procedures, competencies and skills, infrastructure, services, culture and behavior, and applications.
APO03 - managed enterprise architecture	It is essential to balance the various IT architectures used throughout the organization, their relationships, and the guiding principles that have shaped them over time. This will make it possible to achieve operational and strategic goals in a way that is consistent, quick, and cost-effective.
APO07 - managed human resources	Optimize the ability of human resources to meet organizational goals.
APO08 - managed relationships	Manage the appropriate knowledge, abilities, and attitudes to produce better results, boost mutual trust and self-confidence, and efficiently use resources that foster fruitful corporate stakeholder relationships.
APO12 - managed risk	The need to integrate the overall and IT-related organizational risk management and balance the associated costs and benefits.
APO13 - managed security	Maintain information security incidents' effects and frequency within the organization's acceptable level of risk.
BAI01 - managed programs	a) Provide the necessary business value while minimizing the risk of unanticipated delays, expenses, and value degradation. The level of involvement and communication between businesses and consumers impacts this. b) Assure the worth and caliber of project and program outcomes. Maximize the program's investment portfolio contribution.
BAI02 - managed requirements definition	Developing ideal solutions that satisfy the organization's requirements while reducing risk is essential.
BAI03 - managed solutions identification and build	a) Ensure agile and scalable delivery of digital products and services. b) Identify the business procedures, technological advancements, and workflows supporting the organization's operational and strategic objectives.
BAI05 - managed organizational change	Prepare for business transformation with stakeholders, make commitments, and lower the risk of failure.
BAI06 - managed IT changes	Provide for the quick and trustworthy distribution of modifications to businesses.
BAI07 - managed IT change acceptance and transitioning	Lessen the likelihood that a changing environment would suffer harm, compromising its stability or integrity.
BAI10 - managed configuration	a) Give adequate asset information to enable efficient service management. b) Evaluate how changes will affect things and handle service incidents.
BAI11 - managed projects	a) Provide the intended project results while lowering the likelihood of unanticipated delays, expenses, and value erosion through enhancing business and end-user communication and participation. b) Assure that project results are valuable and high-quality and optimize their contribution to the specified program and investment portfolio
DSS01 - managed operations	Delivering planned IT operational goods and services.
DSS02 - managed service requests and incidents	a) Rapidly answering user questions and incidents will help you track enhanced productivity and reduce disruption. b) Investigate changes' effects and handle service occurrences. c) In the event of an incident, respond by resolving user requests and restoring services.
DSS03 - managed problems	Increasing availability and service levels, lowering costs, improving customer convenience and happiness by reducing the frequency of operational issues, and identifying root causes as a problem-solving component are all desirable outcomes.
DSS04 - managed continuity	In a substantial disruption, immediately adjust, resume business operations, and keep resources and information accessible at levels the organization can tolerate (e.g., opportunities, threats, requests).
DSS05 - managed security services	Reducing the impact of operational information security incidents and vulnerabilities on the business.
MEA03 - managed compliance with external requirements	It ensures that the company complies with all relevant outside standards.
MEA04 - managed assurance	Provide companies with the tools they need to create and implement successful assurance projects and to use a road map based on a tried-and-true methodology to plan, scope, implement, and monitor assurance reviews.
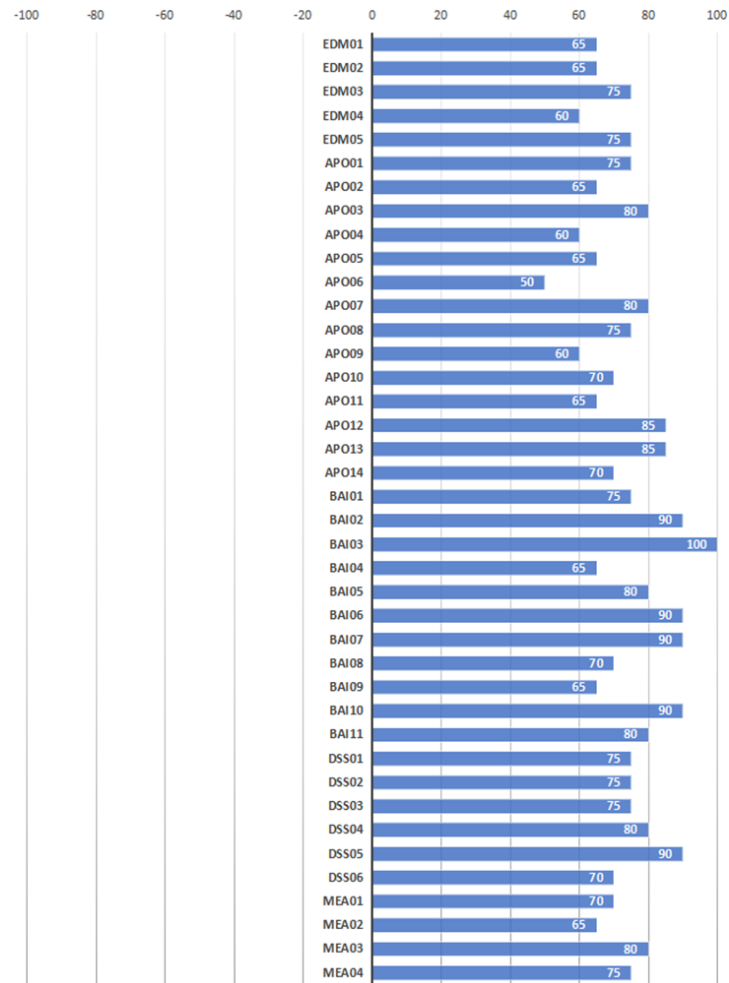
Figure 6. Design governance and management objectives importance

4. CONCLUSION

A good ITG system is needed to carry out the functions and duties of a business organization. Therefore, achievements in the technology sector are due to established strategies and business contexts. The ITG system should be properly managed and implemented to support the organization's business activities by focusing on the core model with a capability level of 4. This research showed that there are 23 core models, including EDM03, EDM05, APO01, APO03, APO07, APO08, APO12, APO13, BAI01, BAI02, BAI03, BAI05, BAI06, BAI07, BAI10, BAI11, DSS01, DSS02, DSS03, DSS04, DSS05, MEA03, and MEA04, which are recommended to be implemented by local government organizations. These models need to be considered as components modified for specific purposes in the focused area of an organization, such as information security, service models, IT roles, DevOps, or specific regulatory compliance.

ACKNOWLEDGEMENTS

REFERENCES

[1] M. Asgarkhani, "The Effectiveness of e-Service in Local Government: A Case Study," *Electronic Journal of e-Government*, vol. 3, no. 4, pp. 157–166, 2005. [Online]. Available: https://www.scribd.com/document/524576729/The-Effectiveness-of-E-Service-in-Local-Government-a-Case#

[2] V. B. R. Mandala and M. S. Chandra, "Cloud Computing Organizational Benefits: A Managerial Concern," 2012. [Online]. Available: https://www.semanticscholar.org/paper/Cloud-Computing-Organizational-Benefits-%3A-A-concern-Mandala-Chandra/8c8c9565b4e74e764cb957fba4ebb51d34f5db6f

[3] W. Hsu, "Conceptual Framework of Cloud Computing Governance Model- An Educational Perspective," *Computer Science*, vol. 7, no. 2, pp. 12–16, 2012. [Online]. Available: https://www.semanticscholar.org/paper/Conceptual-Framework-of-Cloud-Computing-

Governance-Hsu/0d219de1515ddd23f0070aa3bef4a23f846746c1

[4] A. Chaudhuri, "Enabling Effective IT Governance: Leveraging ISO/IEC 38500:2008 and COBIT to Achieve Business-IT Alignment," *The EDP Audit, Control, and Security Newsletter* (*EDPACS*), vol. 44, no. 2, pp. 1–18, 2011, doi: 10.1080/07366981.2011.599278.

[5] C. V. Brown and S. L. Magill, "Alignment of the IS Function with the Enterprise: Toward a Model of Antecedents," *Management Information Systems Research Center, University of Minnesota*, vol. 18, no. 4, pp. 371–403, 1994, doi: 10.2307/249521.

[6] A. C. -Steel, M. Toleman, and W. -G. Tan, "Transforming IT Service Management-the ITIL Impact," in *The Australian Conference on Information Systems*, 2006. [Online]. Available: https://aisel.aisnet.org/acis2006/81

[7] S. De Haes, W. V. Grembergen, A. Joshi, and T. Huygh, "Enterprise Governance of IT," in *Management for Professionals in Enterprise Governance of Information Technology*, vol. 3, no 2, 2020, pp. 15–74, doi: 10.1007/978-3-030-25918-1_2.

[8] M. Asgarkhani, A. C. -Steel, M. Toleman, and M. Ally, "Failed IT Projects: is Poor IT Governance to Blame," in *ACIS 2017 Proceedings*, 2017, vol. 103. [Online]. Available: https://aisel.aisnet.org/acis2017/103

[9] G. J. Selig, "IT Governance-An Integrated Framework and Roadmap: How to Plan, Deploy and Sustain for Improved Effectiveness," *Journal of International Technology and Information Management*, vol. 25, no. 1, pp. 54–76, 2016, doi: 10.58729/1941-6679.1252.

[10] A. H. M. Zaky, A. A. Ragab, M. M. Soliman, and M. A. Ragheb, "Information Technology Governance Effectiveness in Organizations," *The Business and Management Review*, vol. 9, no. 3, pp. 281–289, 2018. [Online]. Available: https://www.researchgate.net/publication/325114935_Information_technology_governanc_effectiveness_in_organizations

[11] W. V. Grembergen and S. D. Haes, "Introduction to the IT Governance and Its Mechanisms Minitrack," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, doi: 10.1109/HICSS.2016.606.

[12] E. Loukis and Y. Charalabidis, "Why do e-Government Projects Fail? Risk Factors of Large IS Projects in the Greek Public Sector: An International Comparison," *International Journal of Electronic Government Research*, vol. 7, no. 2, pp. 59–77, 2011, doi: 10.4018/978-1-4666-2458-0.ch010.

[13] A. Ghildyal and E. Chang, "IT Governance, IT/Business Alignment and Organization Performance for Public Sectors," *Journal of Economics, Business and Management*, vol. 5, no. 6, pp. 255–260, 2017, doi: 10.18178/joebm.2017.5.6.522.

[14] A. O. Tonelli, P. H. D. S Bermejo, P. A. D. Santos, L. Zuppo, and A. L. Zambalde, "IT governance in the Public Sector: A Conceptual Model," *Information Systems Frontiers*, vol. 19, pp. 593–610, 2017, doi: 10.1007/s10796-015-9614-x.

[15] A. Levstek, A. Pucihar, and T. Hovelja, "Towards an Adaptive Strategic IT Governance Model for SMEs," *Journal Theoretical Applied Electronic Commerce Research*, vol. 17, no. 1, pp. 230–252, 2022, doi: 10.3390/jtaer17010012.

[16] L. N. Amali and M. R. Katili, "Identification of influential factors in implementing it governance: A survey study of Indonesian companies in the public sector," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 13, pp. 61–77, 2018, doi: 10.28945/3975.

[17] S. D. Haes and W. V. Grembergen, "Achieving Strategic Alignment and Value" *Enterprise Governance of Information Technology*, Cham, Switzerland: Springer Nature Switzerland AG, 2020, doi: 10.1007/978-0-387-84882-2.

[18] G. Hardy, "Using IT Governance and COBIT to Deliver Value with IT and Respond to Legal, Regulatory and Compliance Challenges," *Information Security Technical Report*, vol. 11, no. 1, pp. 55–61, 2006, doi: 10.1016/j.istr.2005.12.004.

[19] R. R. Peterson, "Integration strategies and tactics for information technology governance," in *Strategies for Information Technology Governance*, pp. 37–80, 2004, doi: 10.4018/978-1-59904-654-9.ch013.

[20] A. Prasad, J. Heales, and P. Green, "Information Technology Resources, Complementaries, and Capabilities: Towards a Deeper Understanding of Leveraging Business Value from IT," in *15th Americas Conference on Information Systems AMCIS*, 2009, vol. 192, pp. 1–10. [Online]. Available: https://aisel.aisnet.org/amcis2009/192

[21] P. Weill and J. W. Ross, "IT Governance, How Top Performers Manage IT Decision Rights for Superior Results," Boston: Harvard Business School Press, 2004. [Online]. Available: https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

[22] S. Ali and P. Green, "Effective Information Technology (IT) Governance Mechanisms: An IT Outsourcing Perspective," *Information Systems Frontiers*, vol. 14, pp. 179–193, 2012, doi: 10.1007/s10796-009-9183-y.

[23] C. -H. Lee, J. -H. Lee, J. -S. Park, and K. -Y. Jeong, "A Study of the Causal Relationship between IT Governance Inhibitors and Its Success in Korea Enterprises," *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 2008, pp. 433-433, doi: 10.1109/HICSS.2008.38.

[24] ITGI, "Board Briefing on IT Governance," 2nd ed. Rolling Meadows, USA: IT Governance Institute, 2003. [Online]. Available: https://www.scribd.com/doc/98700375/Board-Briefing-on-IT-Governance

[25] A. E. Brown and G. G. Grant, "Framing the Frameworks: A Review of IT Governance Research," *Communications of the Association for Information Systems*, vol. 15, 2005, doi: 10.17705/1CAIS.01538.

[26] L. N. Amali, M. R. Katili, S. Suhada, and L. Hadjaratie, "The Measurement of Maturity Level of Information Technology Service Based on COBIT 5 framework," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 18, no. 1, pp. 133-139, 2020, doi: 10.12928/telkomnika.v18i1.10582.

[27] Y. Mahy, M. Ouzzif, and K. Bouragba, "Toward a Shared View of IT Governance," *International Journal of Innovation, Management and Technology*, vol. 7, no. 4, pp. 125–131, 2016, doi: 10.18178/ijimt.2016.7.4.658.

[28] N. K. Kakabadse and A. Kakabadse, "IS/IT Governance: Need For An Integrated Model," *Journals Corporate Governance*, vol. 1, no. 4, 2001, doi: 10.1108/EUM0000000005974.

[29] M. Asgarkhani, "Corporate ICT Governance: A Tool for ICT Best Practice," *The International Conference on Management, Leadership & Governance*, 2013, pp. 1-7. [Online]. Available: https://books.google.co.id/books?hl=id&lr=&id=GKUHBAAAQBAJ&oi=fnd&pg=PA1&dq=M.+Asgarkhani,+%22Corporate+g overnance+ICT:+A+tool+for+ICT+best+practice%22+in+Proceedings+of+the+International+Conference+on+Management,+Lea dership+and+Governance,+2013,+vol.+1,+pp.+1-8.&ots=tKpSlZgDEl&sig=X8pykh1WEAPASOkOUkboW8ccOME&redir_ esc=y#v=onepage&q&f=false

[30] P. Aasi, "Information Technology Governance: The Role of Organizational Culture and Structure," Stockholm University, 2018. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1195170/FULLTEXT01.pdf

[31] ISACA, *Cobit 2019 Framework: Introduction and Methodology*, 2018. [Online]. Available: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

BIOGRAPHIES OF AUTHORS

Lanto Ningrayati Amali ⓘ 🇬 SC ↻ received her Doctoral Degree in Information Technology from the Universiti Utara Malaysia in 2015. Her research interest includes IT Governance, System Planning, and Management of Information System. She has published and presented her research nationally and internationally in IT Governance. She is currently a lecturer in the Faculty of Engineering at the Department of Informatics Engineering, Universitas Negeri Gorontalo in Indonesia. She can be contacted at email: ningrayati_amali@ung.ac.id.

Muhammad Rifai Katili ⓘ 🇬 SC ↻ received his Doctoral Degree in Information Technology from the Universiti Utara Malaysia in 2018. He is a faculty member at the Informatics Engineering Department, Faculty of Engineering, Universitas Negeri Gorontalo in Indonesia. His research interest includes Knowledge Management, Information System, and IT Governance. He can be contacted at email: mrifaikatili@ung.ac.id.

Sitti Suhada ⓘ 🇬 SC ↻ holds a Master in Informatics Engineering from Universitas Hasanuddin, Indonesia. Her research interests include Management Information Systems, Databases, and Data Mining. She is a faculty member at the Department of Informatics Engineering, Faculty of Engineering, Universitas Negeri Gorontalo, Indonesia. She can be contacted at email: sittisuhada@ung.ac.id.