Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 4 (2023) pp: 20-29
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Information System Audit Using COBIT 2019 Framework in Construction Companies

Diza Kurnianty Jamal[1], Haliah[2], Andi Kusumawati[3*]
[1]*Department of Accounting, Ujung Pandang State Polytechnic, Indonesia*
[23]*Department of Accounting, Hasanuddin University, Indonesia*

Abstract: *Disruption is the biggest threat to all industry lines in the digital era, including the construction industry. Therefore, PT XYZ, which is a company engaged in construction has utilized information technology to facilitate integrated business management. This study conducted an information system audit to evaluate the condition of information technology governance. Audits are carried out using framework COBIT 2019 with EDM, APO, BAI and DSS domains. This type of research is field research with data collection techniques through questionnaires, interviews and observation. Audit stages are carried out starting from determine the initial scope of audit, increase the scope of audit, conclude the design factor COBIT 2019, evaluate process capabilities and develop improvement recommendations findings. The results obtained indicate that currently the information system at PT XYZ is well established or at the level of capability level 4 (Predictable Process). However, there is a gap between current conditions and what is expected to achieve the target level 5 (Optimizing Process) on all domain processes. Therefore, the companies are recommended to conduct review of each process due to continuous changes.*

Keywords: *Audit, Information System, Governance, COBIT 2019*

R*eceived 25 Mar., 2023;* ***R****evised 05 Apr., 2023;* ***A****ccepted 07 Apr., 2023 © The author(s) 2023.*
P*ublished with open access at* ***www.questjournals.org***

I. INTRODUCTION

In era of globalization, the role of information systems has become one of the keys to organizational success. The information system is a series of components that are interrelated with each other and work together in achieving the goal of collecting data, processing it into information and conveying that information within the organization. The application of information systems as a supporter of organizational success must be balanced with the effectiveness and efficiency of information system management. There are several ways to determine the effectiveness and efficiency of information system management, one of which is to conduct an information system audit.

Information system audit is a process of collecting data and evaluating evidence to provide confidence whether a computerized application system has been implemented correctly, as targeted and has implemented a comparable internal control system. The IS audit process aims to maintain data integrity, protect the security of company assets, increase the effectiveness of system use, and achieve efficiency in organizing computer-based information [1].

Currently, disruption is the biggest threat to all industry lines in the digital era, including the construction industry. According to McKinsey (2016: 4), there are 5 digitalization trends in the construction industry, namely Higher-definition Surveying and Geolocation, Next-Generation 5D Building Information Modeling, Digital Collaboration and Mobility, The Internet of Things and Advance Analytic, and Future-Proof Design and Construction [2]. These five trends must be carried out simultaneously so that IT investments provide more value to the company.

PT XYZ is a company engaged in construction, Engineering, Procurement and Construction (EPC), railways, tourism, trade, property, real estate and infrastructure investment. The company is a large company and of course it will be difficult if the business processes are done manually. Therefore, companies have utilized IT to facilitate integrated business management. However, based on interviews there are obstacles related to access rights, data integrity, and accounting reporting.

The existence of these constraints, it is necessary to evaluate the information system audit. One framework that can be used as an audit standard is framework COBIT 2019 (Control Objective for Information and Related Technology) issued by Information System Audit and Control Association (ISACA). COBIT 2019 was chosen because the system in the company integrates all of its business processes between one project and another and also the head office with activities in its operational areas, so it is important to carry out a thorough audit.

Based on Nachrowi's research (2020) regarding evaluation of governance and management of information technology services using COBIT 2019 and ITIL 4 shows that IT capability level assessment at the Directorate of Institutional Directorate General of Higher Education conveyed 3 processes at level 0 (incomplete), 6 processes at level 1 (initial), 1 process at level 2 (managed) and 1 process level 3 (define). It means that IT governance is still not optimal because it has not reached the expected maturity at levels 4 and 5. Recommendations are obtained after analyzing the value of the gap between the existing capability level and the target level [3].

This study aims to evaluate by carrying out an information system audit to determine the current level of capability (current capability level). Thus, it can be known whether the expected conditions have been achieved or not and determine the right recommendations for improving the construction company's information system according to the existing problems.

II. LITERATUR REVIEW

A. Information System Audit

According to ISACA, Information System Audit is "Process of collecting and evaluating evidence to determine whether information system and information technology environments adequately safeguards assets, maintain data and system integrity, provide relevant and reliable information, achieve organizational goals effectively consume resources efficiently and have in effect internal controls that provide reasonable assurance that operational and control objectives will be meet" [4].

Fitrawansyah (2014) states that "Information system audit is a systematic process of collecting and evaluating evidence to determine that a computer-based information system used by an organization has been able to achieve its goals [5]. An IT audit focuses on the computer-based aspect of an organization's information system and modern systems employ significant levels of technology [6].

B. Information Technology Governance

According to Bianchi et al, Information Technology Governance consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives [7]. Corporate Governance of IT is the system in which the current and future use of IT is directed and controlled to support the organization. The principles of Good Corporate Governance compiled by the National Committee on Governance Policy (2006) include transparency, independence, accountability, responsibility, fairness [8].

C. COBIT 2019 Framework

Daqiqil (2011) states that a framework is a basic contextual structure that is used to solve a problem or complex issues. In the field of software, it is used to describe a system design. Meanwhile, in the field of management, a framework is used to describes a concept that enables the handling of different types of business entities [9]. The framework that can be used to determine IT performance is Control Objective for Information and related Technology (COBIT) 2019 which provides a detailed IT Governance framework and control objectives for management, business process owners, users and auditors to manage IT holistically so that the value optimally provided by information technology can be achieved by paying attention to all aspects of information technology governance, including aspects of people, skills, competencies, services, infrastructure, and applications which are part of the enablers of an information technology governance. COBIT is developed periodically by the Information System Audit and Control Association (ISACA) [10].

III. RESEARCH METHODOLOGY

This research is a type of field research with a descriptive-quantitative approach. The research was conducted by visiting the company PT XYZ directly. Interviews and observations were carried out as a form of preliminary survey to identify problems in the use of information systems. Furthermore, data was collected through respondents' answers using a questionnaire compiled based on the COBIT 2019 framework according to the problem under study. The results of distributing the questionnaires will be managed to produce numbers in the form of IT governance capability levels. The research stages are described as follows:

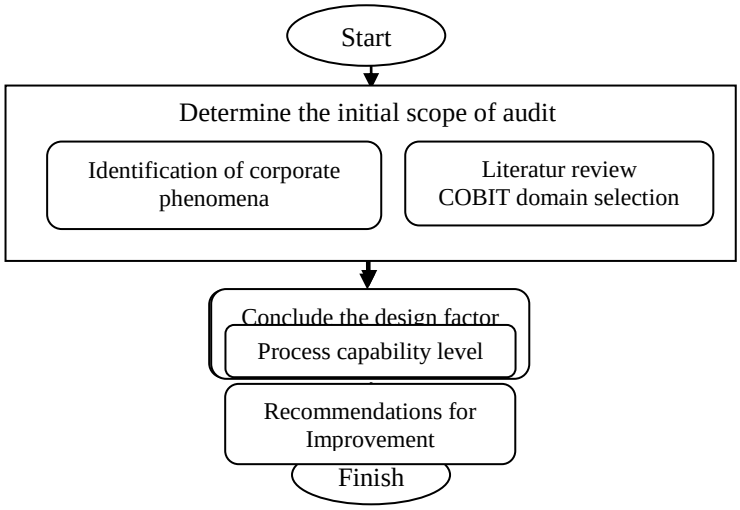

Figure 1: Research Flowchart

IV. RESEARCH RESULT

A. Determine The Initial Scope of Audit

When determining the initial scope of IT governance, There are 11 design factor elements according to the provisions of the 2019 COBIT framework. Design factor 1 (enterprise strategy) describes the company's strategy with PT XYZ based on the four strategies. PT ZYX focuses on client service/stability, so that it is given an importance level value of 5. Next, it is followed by growth/acquisition with an importance value of 4 because this company in its activities places a lot of emphasis on managing company profits.

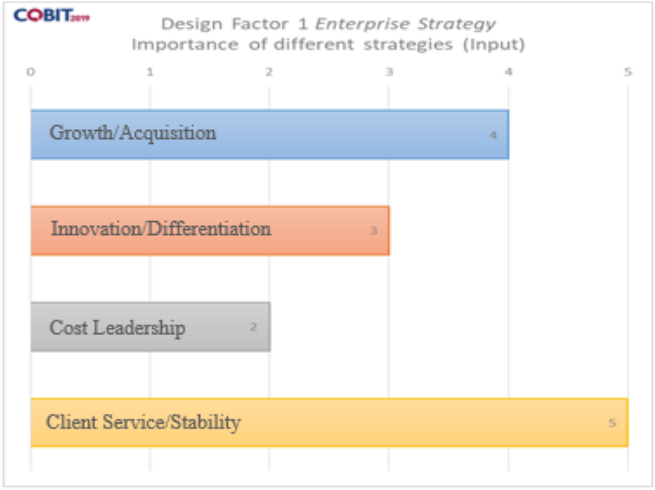

Figure 2: Design Factor 1

Figure 3 shows the results of design factor 2 (enterprise goals). The numbers 1-5 are ratings on the level of importance of each enterprise goal. The higher value indicates the priority of the goals at PT XYZ.

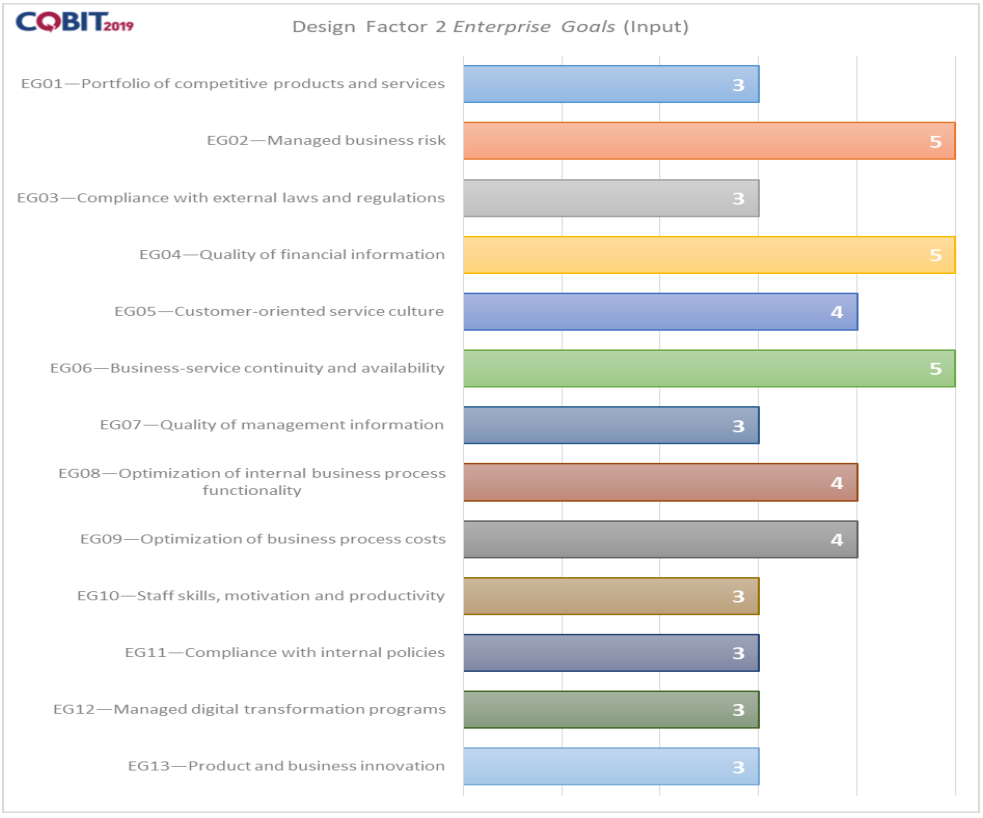

Figure 3: Design Factor 2

Figure 4 shows the results of the likelihood and impact assessment of design factor 3 (risk profile). Each number represents the average value of the importance of the risk to IT. PT XYZ has the highest IT risk in technology-based innovation and data & information management.

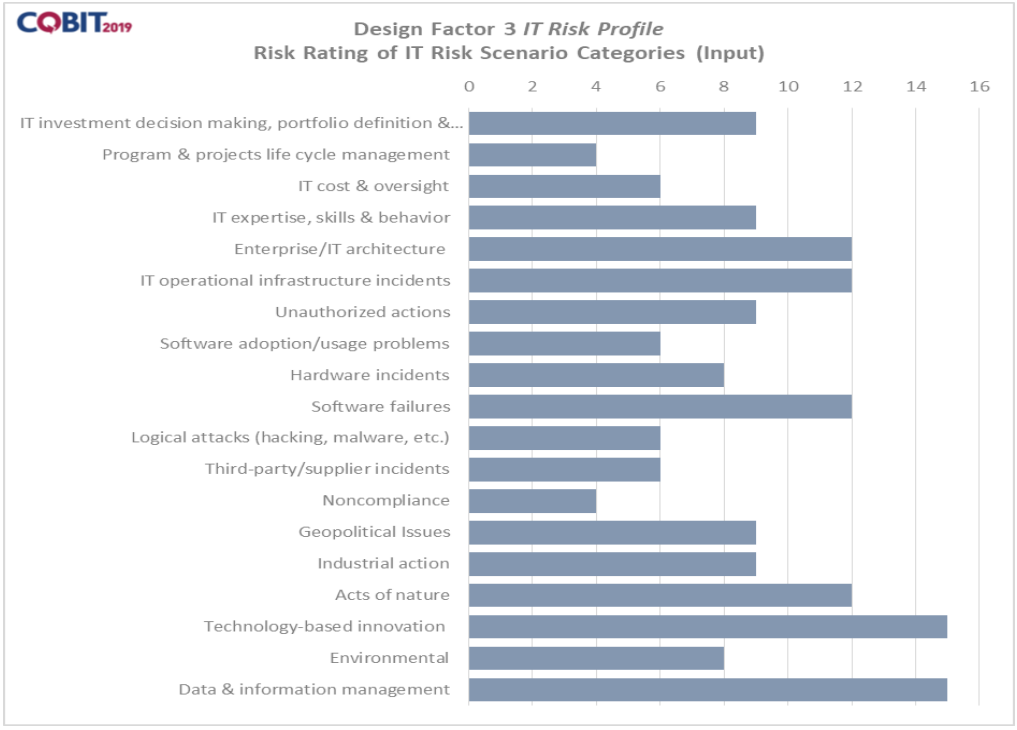

Figure 4: Design Factor 3

Figure 5 shows the results of the assessment of the level of importance of design factor 4 (I&T-related issues). The numbers 0-3 are ratings on the level of importance of the issues to IT. A value of 1 is considered a level of importance not a problem, a value of 2 is considered a problem, and a value of 3 is considered a serious problem.

Figure 5: Design Factor 4

B. Increase The Scope of Audit

In increasing the scope of the governance information system audit, it is necessary to improve the scope of the governance system by addressing design factor elements 5 to 11 based on the COBIT 2019 framework related to threats faced by companies, demands in regulations or requirements, the role of information technology, models of information technology resources , the method chosen to carry out the development of information technology, the strategies carried out to optimize the utilization of information technology, and to take measurements at the company [11].

Figure 6 shows the results of the assessment of the level of importance of design factor 5 (Threat Landscape) in percentage terms. PT XYZ has the same value of 50% at normal and high threat levels.

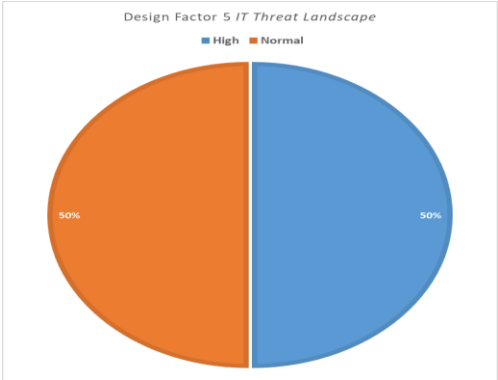

Figure 6: Design Factor 5

Figure 7 shows the results of the assessment of the importance level of design factor 6 (Compliance Requirement) in percentage form. PT XYZ has the highest score of 75% in the normal level of regulatory compliance, complying with industry regulations. PT XYZ is in the construction industry sector, so the regulations applied are related to the business environment and BUMN regulations.

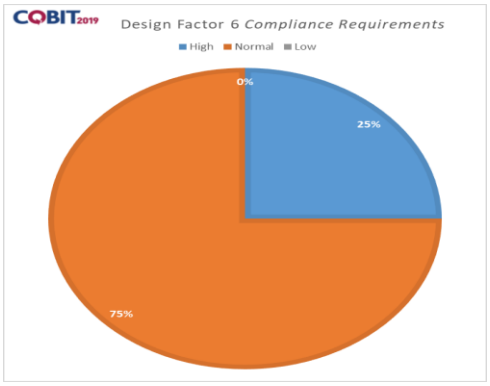

Figure 7: Design Factor 6

Figure 8 shows the design factor 7 (role of IT). The numbers 1-5 are an assessment of the level of influence of the role of IT. A value of 1 is considered very unaffected, a value of 2 is not affected, a value of 3 is moderately affected, a value of 4 is affected, and a value of 5 is greatly affected. PT XYZ has a primary IT role that focuses on being a turnaround which is a supporter in the innovation process, so that it is given a level of influence value of 5.

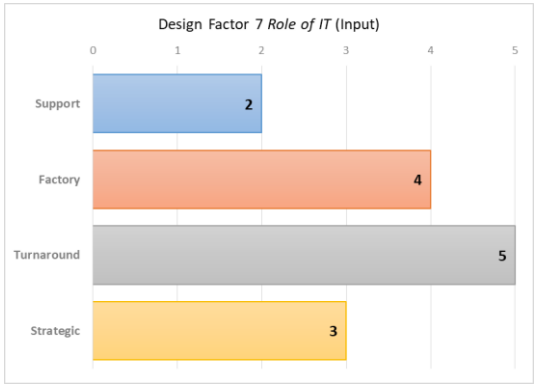

Figure 8: Design Factor 7

Figure 9 shows the design factor 8 (Sourching Model of IT). PT XYZ has a value of 40% on outsourced IT modeler types and 50% cloud. The head office of the type of IT implementation in outsourcing and cloud comes from the PT XYZ head office and branches can provide input to the center in procuring or providing IT services with a 10% value on the type of insourced IT modeler.

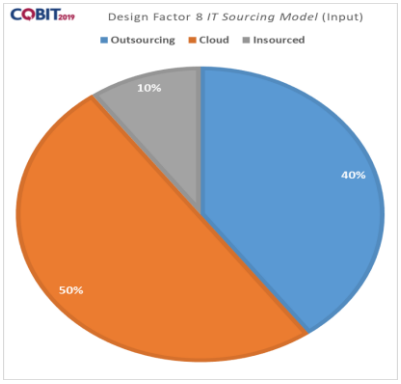

Figure 9: Design Factor 8

Figure 10 shows the results of the design factor 9 (IT Implementation Method). PT XYZ has a value of 50% for the type of application of the Agile method and 40% for devOps because PT XYZ always develops systems and adapts to changes. As for the traditional method, the percentage is 10% for branch offices with limited access.

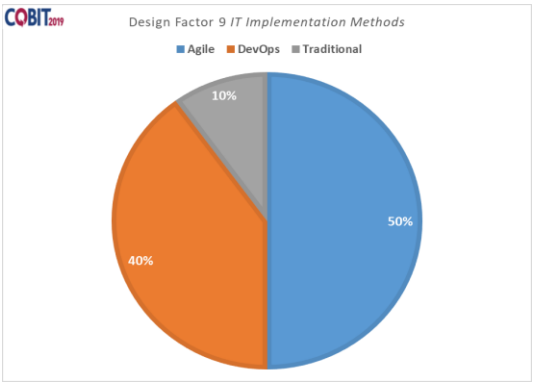

Figure 10: Design Factor 9

Figure 11 shows the results of the design factor 10 (Technology Adoption Strategy). PT XYZ has 60% in the follower category, 30% in the first mover category, and 10% in the slow adopter category. Head office of PT XYZ determines when to take new technology and apply it directly to each of its branches.

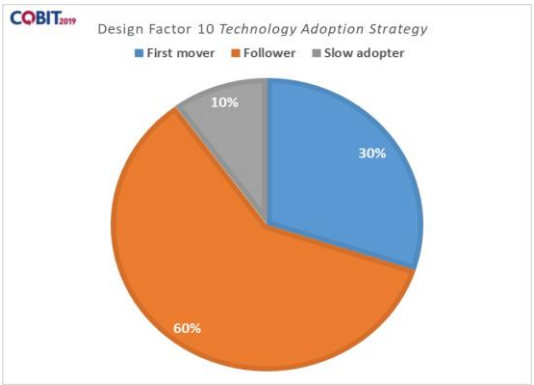

Figure 11: Design Factor 10

In addition, design factor 11 is determined by the number of employees in the company based on COBIT 2019. Companies that are classified as large companies have more than 250 employees. Meanwhile, companies with 50 to 250 employees can be categorized as small and medium companies. PT XYZ is a large company because it has more than 250 employees according to the results of the interviews conducted.

C. Conclude The Design Factor COBIT 2019

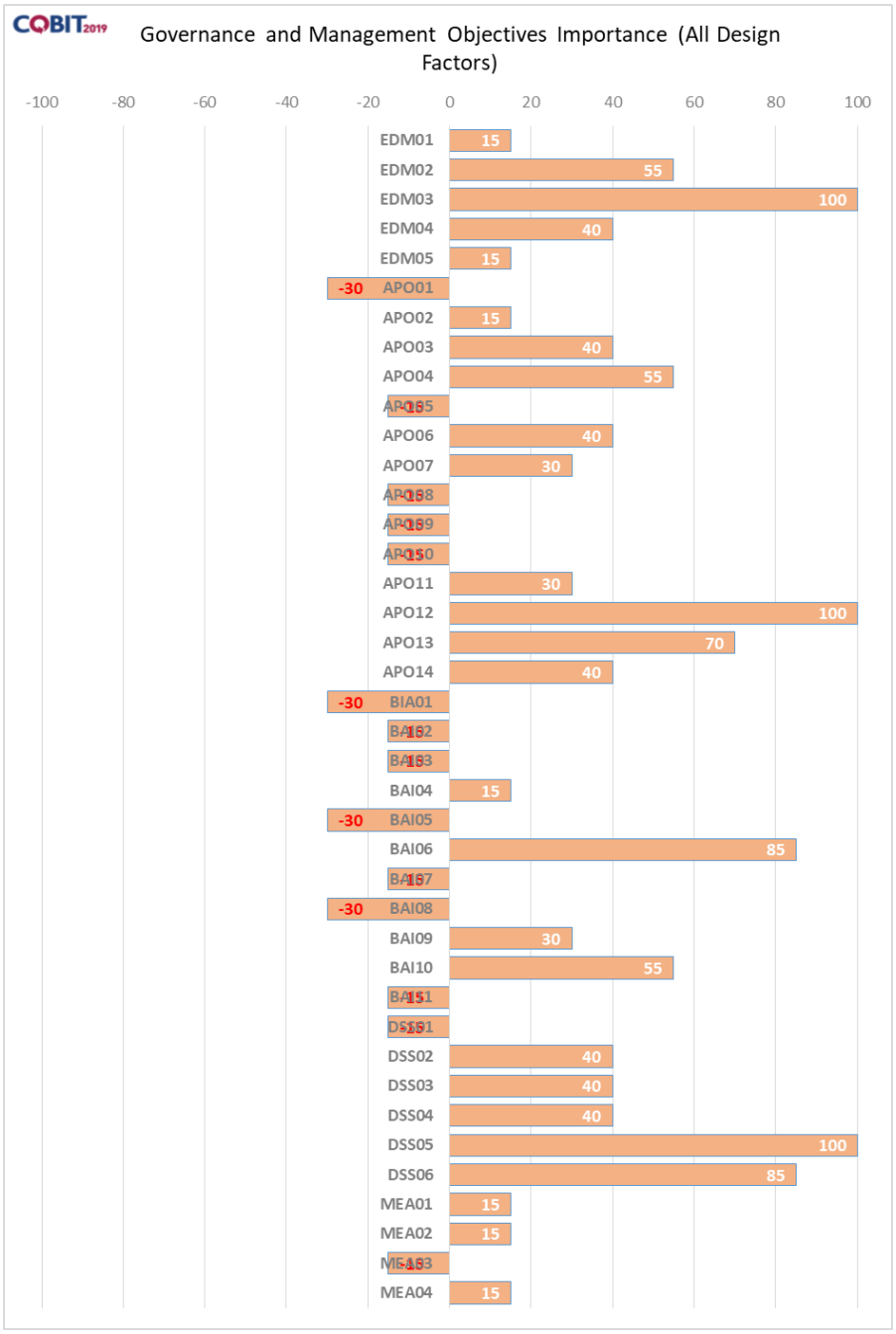

Figure 12: Design Factor Conclution

Figure 12 is a summary of the scope of the governance system at PT XYZ. Where, the core model that has the highest priority is the value ≥ 75 with the level of expectation at level 3 and level 4. Thus, the priority for assessing process capability is the core model EDM03 (Ensured Risk Optimization) of 100, APO12 (Managed Risk) of 100, BAI06 (Managed IT Changes) of 85, DSS05 (Managed Security Service) of 100 and DSS06 (Managed Business Process Controls) of 85.

D. Process Capability Level

After the questionnaire answers were collected, scores were obtained for each activity in the EDM03, APO12, BAI06, DSS05 and DSS06 domains. Next is the stage of giving levels to each sub-process which then produces a gap analysis from the current condition (as is) to the expected condition (to be). The following is the result of determining the value and level of capability contained in each domain:

Domain	Capability Value		Capability Level	
	As is	*To be*	*As is*	*To be*
EDM03.01	3,75	5	4	5
EDM03.03	3,81	4,81	4	5
APO12.01	4,21	4,86	4	5
APO12.02	3,60	5,00	4	5
APO12.03	3,25	4,75	3	5
APO12.04	3,80	4,90	4	5
APO12.05	3,67	5,00	4	5
APO12.06	3,63	5,00	4	5
BAI06.01	4,25	4,92	4	5
BAI06.03	4,42	4,92	4	5
BAI06.04	4,00	5,00	4	5
DSS05.01	5,00	5,00	5	5
DSS05.03	4,33	4,83	4	5
DSS05.05	3,85	4,60	4	5
DSS05.06	4,08	4,58	4	5
DSS06.01	4,11	5,00	4	5
DSS06.02	4,22	5,00	4	5
DSS06.03	4,22	5,00	4	5
DSS06.04	3,83	5,00	4	5
DSS06.05	4,33	5,00	4	5
DSS06.06	4,25	5,00	4	5
Average	4,03	4,91	4	5

Table 1: Capability Level

The results of the capability level assessment for current conditions obtained an average value of all domains 4.03 or at capability level 4 (Predictable Process). As for the conditions that are expected to obtain a value of 4.91 or at capability level 5 (Optimizing Process). There is a difference between the current capability value and the expected value of 0.88.

This condition occurs because the company has determined risks based on overall company goals and preventive and corrective actions, but when there are changes, it still needs to be reviewed to ensure that these actions are still relevant and sustainable. This is because change has become a certainty that occurs continuously with changes that are getting faster and bigger. In addition, the security service process for detected risks is currently good, but still needs to be developed. This is due to technological developments that are increasingly advanced and sophisticated so that threats to information systems will also be greater. Based on the current audit results, it is still at level 4 and needs to be upgraded to level 5 ensured that preventive and corrective action are carried out properly. Therefore, the risk will always change, so that control activities must also be adjusted and improved.

E. Recommendation

Based on the results of information system audits that have been carried out in each COBIT 2019 domain, there are still those who have not reached the capability level expected by the company, level 5 (Optimized Process). These results prove that there is still a level of gap that must be addressed by providing recommendations for improvement so that all domains achieve the expected capability level. The following are recommendations that must be implemented to achieve this level:

1. EDM03 (Ensured Risk Optimization)

Company is recommended to document control details (control matrix) after the process is implemented. This is to make it easier for the company to formulate further improvement steps, for example identifying variations and problems that need attention and forwarding for countermeasures so that risk mitigation measures can truly minimize risk. In addition, the company still needs to take preventive measures so that the risk of loss related to IT whose value is higher than the tolerance threshold can be reduced to the risk tolerance limit that can be accepted by the company. The company also needs to make adjustments after changes in risk appetite related to risks that must be maintained or even eliminated when the previous controls were good.

2. APO12 (Managed Risk)

Company is recommended to document the results of preventive and corrective actions to assess the effectiveness and efficiency of these actions. In addition, the company identifies the suitability of performance when there are changes regarding technological innovation in changes in the business environment, including the emergence of new risks when changes are implemented and risk adjustments that must be maintained or even eliminated. Company is advised to identify quantitative objectives in the risk management process in the form of an early warning system to be notified to superiors if the risk is above a predetermined threshold.

3. BAI06 (Managed IT Changes)

It is recommended that the company conduct a review of the impact and effectiveness of the changes that have occurred in order to minimize the risks in dealing with these changes. The company should have several alternative plans in order to survive and anticipate failures that occur due to change. So that when these changes occur, the company already has the ability to deal with all the advantages and disadvantages of these changes with controls and systems that have been prepared carefully.

4. DSS05 (Managed Security Services)

The company is recommended to conduct a review of the security of user services to monitor and assess whether the continuous improvement in the effectiveness of information security procedures and policies is appropriate or not. The company still has to control the change process related to security services. In this case, the company identifies suitability between preventive and corrective actions with risk after changes in the risk management process.

5. DSS06 (Managed Business Process Control)

The company is recommended to continue to make adjustments between preventive and corrective actions with adjusted risks after changes in the risk management process. This affects the company's control activities that when the risk changes, the control activities must also be adjusted. When there is a business information process error, it is necessary to report it in a timely manner to analyze the root cause of the problem. Improvements are made both by incremental advances in existing business processes and by innovation using new technologies and methods.

V. CONCLUSION

Information system audit at the construction company PT XYZ using the COBIT 2019 framework, there are 5 domains that are in accordance with the company's current conditions, EDM03, APO12, BAI06, DSS05 and DSS06. The audit results show that currently the information system at PT XYZ is well established or at capability level 4 (Predictable Process). This means that the process that has been set is currently operating properly and within the limits that have been determined to achieve the results of the process. However, the capability level is expected to be at level 5 (Optimizing Process) for all domain processes. The existence of these gaps, the company is recommended to conduct a review of each process due to continuous changes so that the risks to the development of information technology are also increasing. Management is required to continue to make adjustments to these developments. So that in a sustainable manner, the process can be implemented and synergized properly and is able to provide the results expected by the company.

REFERENCES

[1]. Weber, Ron. Information System Control and Audit. New Jersey: Prentice Hall. 1999: p. 11-13.
[2]. McKinsey. Imagining Construction's Digital Future. Research Report. Singapura: McKinsey Productivity Sciences Center. 2016, p.4-8.
[3]. Nachrowi, Erika et al. Evaluation of Governance and Management of Information Technology Services Using COBIT 2019 and ITIL 4. Resti Journal (System Engineering and Information Technology). 2020. 4(4): p. 764-774.
[4]. ISACA. CISA Review Manual 2006 (CISA-Certified Information Systems Auditor). USA. 2006.
[5]. Fitrawansyah. Fraud & Auditing. Jakarta: Mitra Wacana Media. 2014: p. 61.
[6]. J. A. Hall. Information Technology Auditing and Assurance. Third Edition. South-Western. Cengage Learning. 2011.
[7]. Bianchi, Rui Dinis Sousa and Ruben P. Information Technology Governance for Higher Education Institutions: A Multi-Country Study. Informatics. 2021. 8(26): p. 1-28.
[8]. Amaliah, Haliah and Syarifuddin Rasyid. The Effect of Enterprise Risk Management and Financial Performance on Firm Value With Good Corporate Governance As A Moderation Variable. Quest Journals of Research in Business and Management. 2022. 10(6). p. 18-26.
[9]. Daqiqil, Ibnu. Framework Codeiqniter. Pekanbaru. 2011.
[10]. ISACA. COBIT 2019 Framework: Introduction and Methodology. USA. 2018.
[11]. Bayastura, S. F., Krisdina, S., & Widodo, A. P. Analysis and Design of Information Technology Governance Using the Cobit 2019 at PT . XYZ. Jiko. 2021. 4(1): p. 68–75.