G-Tech : Jurnal Teknologi Terapan
Volume 7, No. 4, Oktober 2023, hal. 1391-1400
E-ISSN: 2623-064x | P-ISSN: 2580-8737

Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry

Saul Carlos Immanuel Simatupang[1], Melissa Indah Fianty[2]✉

[1, 2] Department of Information System, Faculty of Engineering & Informatics, Universitas Multimedia Nusantara, Indonesia

Informasi Artikel

Riwayat Artikel

Diserahkan : 24-08-2023
Direvisi : 01-09-2023
Diterima : 02-09-2023

ABSTRAK

Perusahaan yang bergerak di bidang jasa dan solusi teknologi informasi terdapat permasalahan Standar Operasional Prosedur (SOP) untuk mendokumentasikan risiko TI. Selain itu, terjadi downtime sistem di server lokal, yang mengakibatkan kehilangan data untuk catatan karyawan, data keuangan, data inventaris, dan data pembelian. Dilakukan pengukuran tingkat kapabilitas tata kelola TI perusahaan, dengan kerangka kerja COBIT 2019 dengan fokus pada area operasional dan keamanan. Hasil pengukuran tingkat kapabilitas untuk proses APO12 menunjukkan telah mencapai level 2, dengan target level 3, proses DSS01 sudah mencapai level 3, memenuhi target level kapabilitas, sedangkan proses DSS02 mencapai level 2 dengan target level 3. Hal ini menunjukkan kesenjangan 1 level dalam proses APO12 dan DSS02. Rekomendasi yang diberikan kepada perusahaan adalah berkonsentrasi pada manajemen risiko, menemukan keseimbangan antara biaya dan manfaat mengelola risiko terkait TI.

Kata Kunci:

Tingkat Kemampuan, COBIT 2019, Tata Kelola Teknologi Informasi

Keywords **:**

Capability Level, COBIT 2019, IT Governance

ABSTRACT

The company engaged in services and information technology solutions is facing issues with Standard Operating Procedures (SOPs) to document IT risks. Additionally, there has been system downtime on the local server, resulting in data loss for employee records, financial data, inventory data, and purchase data. An assessment of the company's IT governance capability is conducted using the COBIT 2019 framework, focusing on operational and security areas. The results of the capability assessment for the APO12 process indicate that it has reached level 2, with a target of level 3. The DSS01 process has already achieved level 3, meeting the target capability level, while the DSS02 process has reached level 2 with a target of level 3. This demonstrates a 1-level gap within the APO12 and DSS02 processes. The recommendation provided to the company is to concentrate on risk management, finding a balance between the costs and benefits of managing IT-related risks.

***Corresponding Author*:**
Melissa Indah Fianty
Information System Department, Faculty of Engineering & Informatics, Universitas Multimedia Nusantara Provinsi Banten, Indonesia
Jl. Boulevard, Gading Serpong, Kel. Curug Sangereng, Kec. Kelapa Dua, Kab. Tangerang, Provinsi Banten, Indonesia
Email: melissa.indah@umn.ac.id

INTRODUCTION

Technological developments support the implementation of business processes that promise very high efficiency and productivity values. Information technology (IT) in an organization must continuously adapt to changing internal and external data needs (Maria, 2018). In implementing the strategy and goals of business organizations, information technology does not always run smoothly and according to plan. To support the successful implementation of IT in an organization, it is necessary to improve IT governance (Putra, 2020). IT is governance provides organizations with guidance for managing IT assets and making decisions to achieve business goals. By measuring IT management, organizations can improve the quality of IT services, minimize risks, and optimize the performance of IT services so that organizational goals can be achieved in an efficient and structured manner (Fajarwati, 2018) (Ambarita, 2022). This encourages the company to improve the governance of information technology services to minimize the risks associated with the operational activities of the company.

The company is engaged in services and services that apply information technology in various business industries such as finance, manufacturing, and logistics. The company focuses directly on developing systems for websites, mobile, both Android and iOS, as well as providing services such as operating and ensuring system availability according to business needs, maintenance, procurement and repair of hardware and software, maintenance and maintenance of network devices, configuring and providing internet services as well as designing and managing on the infrastructure side of IT devices both from devices and data center media. However, the process of repairing user problems requires adequate IT equipment infrastructure to provide convenience in making requests for repairs to user problems and affecting the course of the company's business operations.

Issues regarding information technology governance within the company encompass the lack of standardized procedures overseeing the documentation of IT risks within both the internal and external business landscapes. Complications arise from the utilization of on-premises servers due to malware or viruses, along with inadequate data security measures leading to the compromise of both client and company data (Iswara, 2018). Until now, the local server at the company is still experiencing system downtime that originates from other party errors or human errors that impact the company's and client's business operations (ISACA, COBIT® 2019 Framework: Introduction and Methodology, 2018).

Considering the issues at hand, it's essential to promptly address these concerns due to the company's primary concentration on providing services. If there remains a misalignment between business operations and the utilization of information technology, inherent risks are bound to arise. Numerous frameworks are available for evaluating a company's capacity to manage information technology effectively (ISACA, COBIT® 2019 Design Guide: Designing an information and technology governance solution, 2018). Given these challenges, the company necessitates a framework for gauging the extent of its information technology governance capabilities (Anjelina, 2021) (Herliani, 2021) (Aditya, 2019).

According to ITGI and ISACA, IT governance is categorized into five elements, which comprise IT Strategic alignment, IT value delivery, IT risk management, performance assessment, and IT resource oversight. Based on the three frameworks discussed previously, an assessment was made between the three frameworks for the five components of IT governance, and the result is that COBIT is a complete framework for measuring IT governance (Almunadia, 2019) (Fianty D. S., 2022) (Information, 2021). The research will make use of the COBIT 2019 framework, an established system designed to facilitate proficient corporate governance across business and technological domains while enhancing resource utilization. Furthermore, this study aims to assess the company's competence in executing IT processes. This assessment of capability aligns with the approach taken in numerous preceding studies, employing the COBIT 2019 framework for measurement (Insani, 2022) (Maskur, 2018).

Hence, this research employs the 2019 COBIT framework, focusing on operational and security aspects within the company, particularly in the context of its services and service-related

challenges. These challenges encompass issues like the absence of standardized operating procedures governing the documentation of IT risks across both internal and external business domains, instances of data loss involving client and company data, as well as local server failures necessitating accurate and suitable resolutions. The 2019 COBIT framework is utilized in this study to identify challenges and requirements, aiming to ascertain the company's proficiency in managing IT. The evaluation approach has shifted from maturity levels to employing the 2019 COBIT Process Assessment Model, specifically the concept of capability levels (ISACA, isaca.org, Sertification, 2020). The results of this measurement will be used as a basis for recommendations and evaluation of information technology performance so that they become material for standardization and recommendations for improving the quality of services and services at the company (Rahayu, 2020).

RESEARCH METHOD

The research was conducted by first developing scenarios using the COBIT 2019 framework. Data were obtained from interviews (Fianty W. H., 2022). In Figure 1, the following are the steps carried out during this research process:

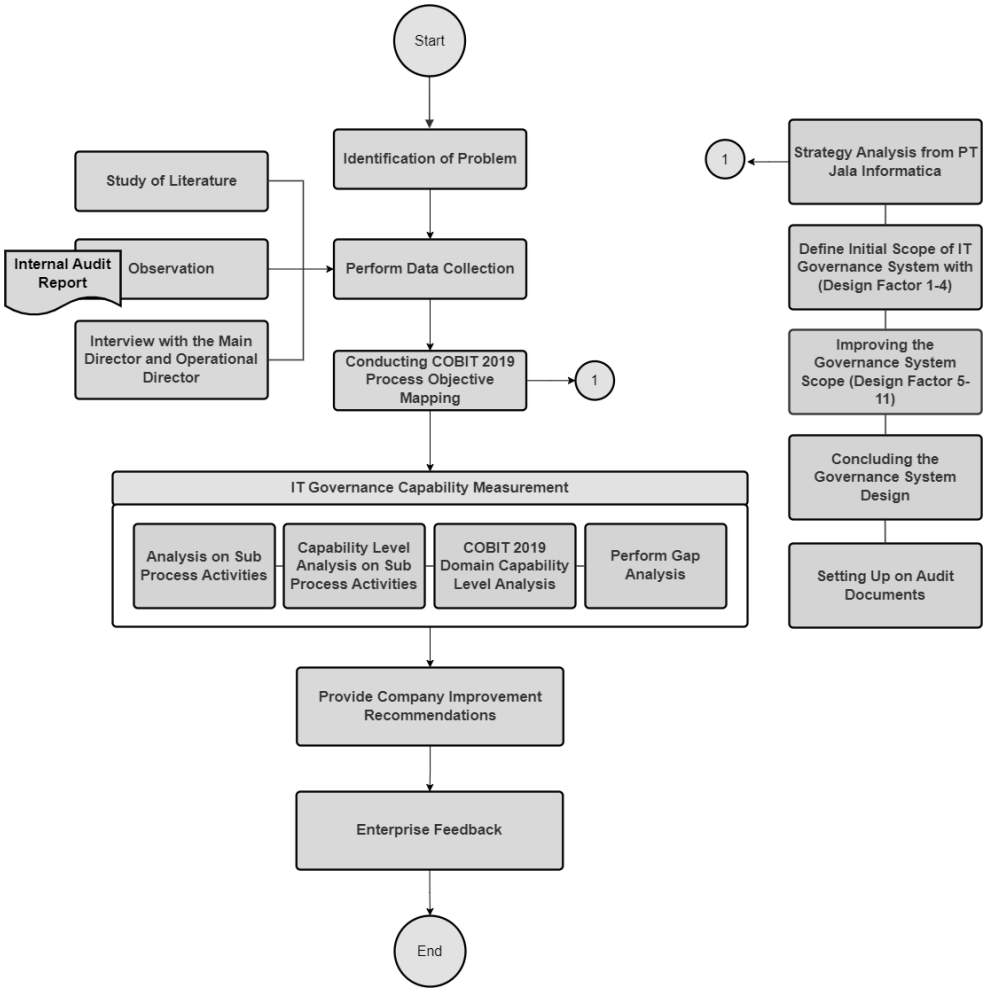

Figure 1. Research Flowchart

Identification of Problems

During the phase of identifying issues, comprehending the requirements of stakeholders concerning the company's strategy, goals, and existing risk landscape, the process of problem identification is executed through a combination of online and in-person interviews with the President Director and Director of Operations. Moreover, an understanding of the company's stakeholders' needs is acquired by observing data on the internal server.

Data Collection

At the data collection stage, a literature review of related books and journals is carried out to better understand COBIT 2019, especially for security and operational issues which can be used as a reference source, make direct observations of companies to find out company operational activities and analyze data on lost clients, server companies and analysis findings in internal audit reports and other supporting documents. Subsequently, interviews are carried out with company representatives to ascertain the prevalent issues and offer an evaluation of the audit documents corresponding to each objective.

COBIT 2019 Process Objective Mapping

Moving to the following phase, the aims of the 2019 COBIT processes will be established, drawing from insights garnered through interviews with the President Director and Director of Operations concerning the company's challenges, specifically focusing on security and operational aspects. The mapping process starts from the design factor in determining the initial IT governance scope with DF 1-4, data input is carried out in the COBIT 2019 toolkit, and after that the scope of governance is refined for DF 5-11, and the factor set design ends with data that have been submitted to generate objectives or domains in the 2019 COBIT process.

IT Governance Capability Measurement

Once the interview data has been collected, the subsequent step involves assessing the company's IT governance capability. The initial phase entails analyzing the activities of sub-processes. From these processes, a set of questionnaire items will be formulated, intended for distribution to the President Director and the Operations Commissioner. The subsequent phase involves evaluating the capability level of sub-process activities, utilizing the directives provided by COBIT 2019 for capability levels. Moving on to the third stage, each sub-process within every goal domain of COBIT 2019 will be evaluated, resulting in the creation of a rating scale, which adheres to the guidelines outlined in the 2019 COBIT framework. Finally, the fourth stage encompasses conducting a Gap Analysis to determine the desired level of capability that the company aims to achieve. This will unveil the disparity between the current capability level and the targeted level of proficiency.

Provide Recommendations

Derived from the outcomes of the IT governance measurement process, this study will generate suggestions for enhancements aimed at resolving company challenges and addressing them effectively, thereby enhancing the quality of IT governance.

Enterprise Company

Drawing from the provided recommendations, the company will initiate a review process to ensure the sufficiency and effectiveness of these suggestions in aiding the business to confront and mitigate the encountered challenges.

RESULT AND DISCUSSION

Identification of Problems

In the past year, the company experienced the first problem, experiencing 11 errors on the local server for client data on the HRIS page, the second problem, losing data contents from the company's server 7 times because the company was still using the on-premise server and the last problem, there is no SOP that regulates IT risk documentation in the internal and external business environment. This causes delays in the company's and client's day-to-day operational activities such as disturbances in employee data, salary information, and attendance records. In addition, it has an impact on the company's operational activities which lasts for seven days due to the absence of data completeness and recovery of client data for about two months as well as vulnerabilities to

data security failures, decreased IT performance, loss of reputation, loss of trust with clients, and constraints in adopting innovative technology.

Conducting 2019 COBIT Process Objective Mapping

In the company's endeavor to execute IT governance assessments, the COBIT 2019 framework is employed for evaluating the proficiency in each IT governance procedure. The assessment of IT governance proficiency within an organization commences with the requirement of objectively aligning the COBIT processes. To facilitate this objective alignment of COBIT processes, the COBIT 2019 design toolkit comes into play. Within this toolkit, measurements will be conducted for each design element.

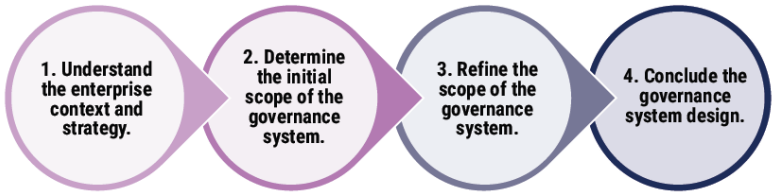

Figure 2. COBIT 2019 Governance Design Flow
(ISACA, COBIT® 2019 Framework: Introduction and Methodology, 2018)

Figure 2 shows the COBIT 2019 governance workflow that guides how companies can implement COBIT 2019 in a structured and systematic manner. By following these steps, companies can manage and improve corporate information technology governance by business goals.

Understanding Context and Company Strategy

In this step, the company's external and internal context will be summarized by first understanding the company strategy used, the company's goals to be achieved, possible IT risk profiles, and IT-related problems currently experienced by the company. The corporate strategy used by the company focuses on service innovation for clients.

Defining the Initial Scope of the Governance System

During this phase, the preliminary extent of the governance system is established using the toolkit furnished by COBIT 2019, with the intent of outlining domain objectives. Subsequently, the process advances by considering the aspects encompassed within design factors 1 to 4, aimed at uncovering the enterprise strategy, enterprise objectives, IT risk landscape, and IT-related challenges. This is followed by an exploration of design factors 5 to 11, which serve to identify facets such as the IT Threat Landscape, Compliance Requirements, the role of IT, IT sourcing approach, strategies for IT implementation, methods of technology adoption, and the scale of the enterprise.

Conclusion Design Factors

Upon scrutinizing and defining objectives through the utilization of Design Factors (DF1 - DF11), the subsequent step entails formulating a design for the company's governance system. This design encompasses pivotal governance and management objectives prioritized to finalize the governance system blueprint and attain the goals stipulated within COBIT 2019. (ISACA, COBIT® 2019 Design Guide: Designing an information and technology governance solution, 2018).

Table 1. Design Factor Conclusions

Process	Score (%)
APO12 – Managed Risk	85%
DSS01 – Managed Operations	75%
DSS02 - Managed Service Request and Incidents	85%

Based on the information presented in Table 1, it becomes evident that design factors 1-11 have successfully generated objective domains. These domains will be integral in the process of evaluating IT governance capabilities within companies, aligned with the COBIT 2019 guidelines. Within these guidelines, the process objectives that demonstrate values of 75 or higher are those associated with adjusted design factors, specifically APO12 - Managed Risk, DSS01 - Managed Operations, and DSS02 - Managed Service Requests and Incidents. These three objective domains achieve a score of 85, indicating their exceeding of the threshold of 75. The comprehensive review of the design factors reveals that these three domains are grappling with challenges and issues. The subsequent phase involves the collection of data through interviews and the utilization of the sub-processes of the selected domain activities.

Measuring Capability Level

Based on the results of the assessments that have been carried out obtained from interviews with the President Director and the Director of Operations, the following is the average calculation result for each objective and level of ability:

1. APO 12 – Managed Risk

The objective of the APO12 process is to fuse I&T-related enterprise risk management with the broader enterprise risk management (ERM) framework while effectively weighing the expenses and advantages associated with the management of I&T-related enterprise risks. Presented below are the findings pertaining to the assessment of capability within the APO12 process:

Table 2. APO12 Calculation Results Level 2

Process	Score	
APO12.01	47,5%	
APO12.03	65%	
APO12.05	25%	
Capability Level Results	Total	137,5%
	Average / 3	45,8%

Table 2, shows the average yield divided by three is 45.8% which is included in the Partially achieved criteria the so. That the APO12 process at the company is at level 2, so the company cannot continue to level 3 because the calculation results do not reach 85%. This is because the company has not fully optimized risks and has taken advantage of strategic opportunities that can provide profit and growth for the company's business.

2. DSS01 – Managed Operations

The primary objective of the DSS02 process is to enhance productivity and mitigate disruptions by promptly addressing user inquiries and incidents. This involves evaluating the repercussions of changes, managing service-related incidents, addressing user requests, and efficiently restoring services in response to incidents. The subsequent section presents the outcomes derived from the measurements conducted within the DSS02 process.

Table 3. DSS01 Process Calculation Results Level 2 and 3

Process	Score Level 2		Process	Score Level 3
DSS01.01	89%		DSS01.01	75%
DSS01.03	90%		DSS01.02	73,3%
DSS01.04	77,6%		DSS01.03	73,25%
DSS01.05	79%		DSS01.04	71,6%
Capability Level Results	Total	335,6%	DSS01.05	75%
			Total	368,15%
	Average / 4	83,9%	Average / 5	73,63%

Table 3 displays an average output amounting to 73.63%, aligning with the criteria denoting "Largely Achieved." Meanwhile, in the context of the company's DSS01 - Managed Operations process, it stands at level 3. This implies that the DSS01 process at the company has successfully met its target at level 3, substantiated by a calculation outcome of 85%.

3. DSS02 – Managed Service Requests and Incidents

The primary objective of the DSS02 process is to enhance productivity and minimize disruptions by swiftly addressing user inquiries and incidents, as well as evaluating the implications of changes. This involves managing service-related incidents, fulfilling user requests, and promptly restoring services in response to incidents. Presented below are the measurement outcomes derived from the evaluation of the DSS02 process:

Table 4. DSS02 Level 2 Process Calculation Results

Process	Score	
DSS02.02	58,6%	
DSS02.03	56%	
DSS02.04	58,3%	
DSS02.05	48,75%	
DSS02.06	57,5%	
DSS02.07	15%	
Capability Level Results	Total	294,15%
	Average / 6	49%

Table 4 displays the average outcomes divided by 49%, falling within the "Partially Achieved" category. Consequently, the DSS02 - Managed Service Request and Incidents process within the company stands at level 2. Consequently, the company cannot progress to level 3 due to the calculation results not attaining the 85% threshold. This situation arises from the company's failure to implement efficient IT incident management and capitalize on strategic opportunities that have the potential to yield benefits and foster business growth.

Gap Analysis

Derived from the conducted interviews with the President Director and Operational Director of the company, and taking into account their preferences as discussed, a specific target capability level is established. The subsequent table illustrates the gap analysis for the domains of company APO12, DSS02, and DSS01:

Table 5. Gap Analysis

Objective	Expected Level of Capability	Current Capability Level	Gap Analysis
APO12 – Managed Risk	3	2	1
DSS01 – Managed Operations	3	3	0
DSS02 – Managed Service Requests and Incidents	3	2	1

Presented in Table 5 is an analysis of the disparity between the existing capability level and the desired capability level. This analysis serves the purpose of assisting companies in gauging the effectiveness of their implemented IT governance measures and determining whether they are functioning optimally or necessitate further enhancement. Subsequently, a radar chart is formulated to visually represent the outcomes of each of these processes.

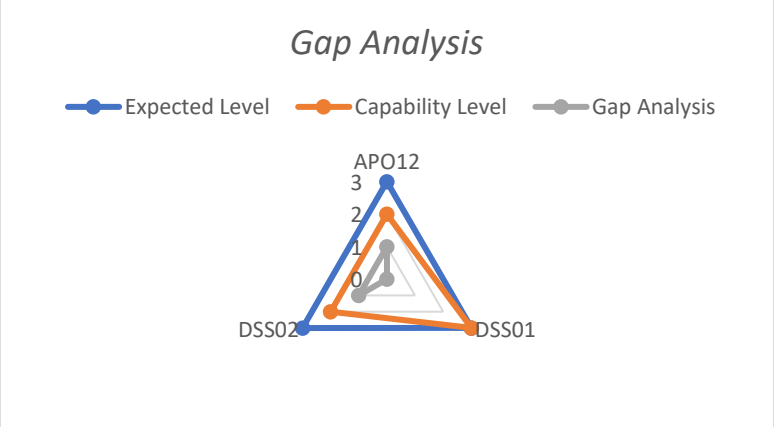

Figure 3. Radar Chart Gap Analysis

Figure 3 illustrates the outcomes stemming from the gap analysis conducted between the anticipated capability level and the company's current capability level for the APO12 process objective. The outcome stands at 45.8%, which corresponds to level 2, signifying that the company has not attained the intended capability level of level 3. Concerning the DSS01 process objective, the achievement stands at 73.63%, indicating that the set target of level 3 has been successfully reached. However, for the DSS02 process objective, the accomplishment is at 49%, indicating an inability to meet the desired capability level of level 3. This essentially implies that both APO12 and DSS02 exhibit a one-level gap between the projected capability and the existing level of proficiency.

Recommendation

After obtaining the results of measuring the level of capability and finding problems and their impacts, the next step is to provide recommendations for improvements to the problems that exist in the company and recommendations for increasing capabilities to be able to move forward level.

Table 6. APO12 Level 2 Process Improvement Recommendations

Process	Activity	Recommendations
APO12.01	Identify and collect relevant data to enable effective identification, analysis, and reporting of IT-related risks.	Companies need to improve employee understanding of IT risks, as well as develop comprehensive IT risk documentation, to reduce the negative impacts that may occur.
APO12.05	Manage operational activities to reduce IT risk to an acceptable level as a basis for assessment.	Companies need to encourage a systematic and systematic approach to managing IT opportunities and risks to achieve optimal profit and growth.

Presented in Table 6 are the suggestions stemming from the APO12.01 and APO12.05 processes. Thesesuggestions pertain to the upkeep of a register containing identified risks and their pertinent attributes. This encompasses anticipated frequency, potential consequences, and corresponding responses. Additionally, it involves documenting the associated resources, capacities, and prevailing control measures connected with risk factors. The given recommendations emphasize that the company should establish swift and comprehensive responses through the employment of well-defined system protocols for handling disruptions or incidents within IT services. Moreover, a robust security system is advised to safeguard both client and company data.

Table 7. DSS02 Level 2 Process Improvement Recommendations

Process	Activity	Recommendations
DSS02.05	Document, implement, and test the identified solution or solutions. Perform recovery actions to restore IT-related services.	The company needs to take effective risk measures, including appropriate security measures, speedy recovery, and precautions against virus attacks, to mitigate any negative impacts that may occur.
DSS02.07	Track, analyze, and report regular IT incidents and fulfilment requests. Check trends to provide information for continuous improvement.	The company needs to take the right actions in handling IT incidents, including repairing infrastructure, increasing security measures, and having an effective recovery strategy to reduce the negative impacts that may occur.

Table 7 shows recommendations from the DSS02.05 and DSS02.07 processes regarding storing, implementing, and testing the identified solution or workarounds and tracking, analyzing, and reporting incidents, and fulfilling requests regularly for future improvements. The recommendation given to the company is to take effective risk measures, including appropriate security measures, and to take appropriate measures in dealing with IT incidents. Researchers provide recommendations for companies according to the findings and the impact on the subdomain.

Order of priority that can be implemented first on DSS02.07 process with 15% companies need to take appropriate action in dealing with IT incidents, including repairing infrastructure, second APO12.05 with 25% companies need to encourage a score of a structured and systematic approach in managing IT opportunities and risks, the third APO12.01 with a score of 47.5% companies need to increase employee understanding of IT risks, then APO12.05 with a score of 48.75% companies need to encourage a structured and systematic approach in managing IT opportunities and risks.

CONCLUSION AND RECOMMENDATION

Conclusion

Based on the findings derived from the conducted research, a comprehensive conclusion can be drawn. The level of corporate IT governance capability has been assessed within the defined objective processes. The APO12 - Managed Risk process attains level 2, achieving a score of 45.8%. In contrast, the DSS01 - Managed Operations process reaches a higher level of 83.9%, successfully meeting the targeted capability level of level 3, with a score of 73.63%. Lastly, the DSS02 - Managed Service Requests and Incidents process stands at level 2, scoring 49%. Significantly, there exists a one-level gap between the existing capability levels within the APO12 and DSS02 processes, which remain at level 2, and the targeted capability level of level 3, as sought by the company.

In total, the company has been provided with 19 recommendations, encompassing seven for the APO12 process and twelve for the DSS02 process. It's noteworthy that the company has shown agreement with all of these recommendations, with the intention of implementing them once the company possesses qualified human resources and attains a stable income.

Recommendation

Companies are advised to carry out the recommendations that have been given in each domain that has findings within a pre-agreed time. Recommendations for increasing the level must be implemented so that the company can achieve the desired target level and it is hoped that for further research to get a more comprehensive perspective, it is recommended to involve participants involving operational staff in further research that can be carried out to measure the success of COBIT 2019 implementation in achieving IT performance, increased compliance, reduced risk, or increased efficiency. This approach will provide real evidence of COBIT 2019's contribution to organizations.

ACKNOWLEDGEMENT

The research has been conducted seamlessly, and credit is due to the assistance and backing provided by Universitas Multimedia Nusantara. Gratitude is extended for the valuable aid and support extended throughout the process of composing this article.

REFERENCES

Maria, A. S. (2018). Analisa Tingkat Kepuasan Pengguna Dan Tingkat Kepentingan Penerapan Sistem Informasi Djp Online Dengan Kerangka Pieces. *Khazanah Inform. J. Ilmu Komput. Dan Inform, 3*(2), 88.

Putra, A. S. (2020). Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan COBIT 2019 (Studi Kasus: Laboratorium Kalibrasi BSML Regional II. *J. Fasilkom, 10*(3), 241-247.

Fajarwati, S. a. (2018). Evaluasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5. *JUITA J. Inform, 6*(2), 73-80.

Ambarita, R. &. (2022). Pengukuran Tingkat Risiko Terhadap Kapabilitas Tata Kelola Teknologi Informasi Berdasarkan Framework COBIT 5. *Jurnal Tekno Kompak, 16*(1), 97.

Iswara, I. D. (2018). Analisis dan Perancangan Helpdesk Ticketing System Untuk Mengelola Tindakan Perbaikan Perangkat Komputer Dan Jaringan Pada PT.Len Industri (Persero) Menggunakan Metodologi Pdca (Plan-Do-Check-Action). *e-Proceeding of Engineering, 5*(3), 7149.

ISACA. (2018). COBIT® 2019 Framework: Introduction and Methodology.

ISACA. (2018). COBIT 2019 Design Guide: Designing an information and technology governance solution.

Anjelina, M. (2021). Pengukuran Kemampuan Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 2019 Pada PT. Mobile Indonesia.

Herliani, M. (2021). Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019.

Aditya, M. D. (2019). Perbandingan COBIT 2019 dan ITIL V4 Sebagai Panduan Tata Kelola dan Management IT. *Jurnal Computech & Bisnis, 13*(2), 100-105.

Almunadia, T. F. (2019). Perancangan Enterprise Architecture Pada Bidang Agroforestry Menggunakan Metode Togaf 9.1 Adm. *J. Resti (Rekayasa Sist. dan Teknol. Informasi), 3*(2), 210-215.

Fianty, D. S. (2022). Measurement of Capability Level Using COBIT 5 Framework (Case Study: PT Andalan Bunda Bijak). *Ultim. InfoSys J. Ilmu Sist. Inf, 13*(2), 68-76.

Information, S. U. (2021). "Pengukuran Tingkat Kematangan Ketersediaan Layanan Akademik pada Sistem Informasi Akademik Menggunakan COBIT 4.1. *e-Jurnal JUSITI (Jurnal Sist. Inf. dan Teknol. Informasi), 82*(2), 155-166.

Insani, S. A. (2022). Implementasi Framework COBIT 2019 Terhadap Tata Kelola Teknologi Informasi Pada Balai Penelitian Sungei Putih. *Jurnal Teknik Informatika Kaputama (JTIK), 6*(1).

Maskur, M. A. (2018). Implementasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Di BPMPTSP Bone Bolango. Masyarakat Telematika Dan Informasi. *Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 8*(2), 109. 7.

ISACA. (2020, July). *isaca.org, Sertification*. Retrieved Maret 6, 2023, from https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-the-iia-2019-guiding-principles-of-corporate-governance.

Rahayu, N. M. (2020). Audit Sistem Informasi Akademik Menggunakan metode COBIT 5. *Jurnal Teknologi Informasi dan Pendidikan, 13*(1), 117-123.

Fianty, W. H. (2022). Analyzing Level of International Humanitarian Law Knowledge and its Compliance Through Military Simulation Game. *Ultim. InfoSys J. Ilmu Sist. Inf., 14*(2), 2.

Consulting, L. C. (2021). IT Governance 적용 사례. *Gov. An Int. J. Policy Adm*, 1-16.

ISACA. (2018). COBIT® 2019 Design Guide: Designing an information and technology governance solution.