G-Tech : Jurnal Teknologi Terapan
Volume 7, No. 4, Oktober 2023, hal. 1498-1508
E-ISSN: 2623-064x | P-ISSN: 2580-8737

Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector

Robertus Nanda Christiadi[1], Rudi Sutomo[2]✉

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

Informasi Artikel

Riwayat Artikel

Diserahkan : 29-08-2023
Direvisi : 12-09-2023
Diterima : 17-09-2023

ABSTRAK

Penerapan tata kelola TI dalam perusahaan, termasuk sektor enterprise dan skala BUMN, telah menjadi suatu keharusan yang mendesak di dunia bisnis saat ini. Hal ini stelah ditetapkan oleh Peraturan Menteri Luar Negeri Nomor 2 Tahun 2013, Pasal 2(1), yang mengikat dunia usaha. Keamanan TI menjadi isu krusial dalam sektor korporasi, membutuhkan perhatian serius. Framework COBIT 2019 menjadi alat penting dalam mengukur kematangan tata kelola TI. Pengukuran ini menghasilkan analisis tingkat kapasitas dan kesenjangan yang sangat penting. Hasil pengukuran menunjukkan bahwa subdomain APO12 – Manajemen Risiko, APO13 – Keamanan Terkelola, dan DSS05 – Layanan Keamanan Terkelola memiliki tingkat kematangan pada level 2. Namun, sangat penting untuk mencatat bahwa DSS05 terhenti pada level 2, menunjukkan adanya kesenjangan dalam kebijakan keamanan titik akhir, kebijakan akses, dan pengelolaan log peristiwa dalam insiden TI. Hasil ini menyoroti urgensi perbaikan dan peningkatan dalam tata kelola TI di sektor perusahaan, terutama dalam subdomain DSS05. Untuk menutup kesenjangan ini diperlukan perbaikan segera dalam kebijakan keamanan titik akhir, kebijakan akses, dan log peristiwa dalam insiden TI agar dapat segera teratasi.

Kata Kunci:

Analisis GAP, COBIT 2019, Rekomendasi, Sub-Domain, Tingkat Kapabilitas.

Keywords **:**

Capability Level, COBIT 2019, GAP Analysis, Recommendation, Sub-Domain.

ABSTRACT

Implementing IT governance in companies, including the enterprise sector and state-owned enterprises, has become an urgent necessity in today's business world. This has been stipulated by Minister of Foreign Affairs Regulation Number 2 of 2013, Article 2(1), which is binding on the business world. IT security is a crucial issue in the corporate sector, requiring serious attention. The COBIT 2019 framework is an important tool in measuring IT governance maturity. This measurement produces a very important analysis of capacity levels and gaps. The measurement results show that the subdomains APO12 – Risk Management, APO13 – Managed Security, and DSS05 – Managed Security Services have a maturity level of level 2. However, it is important to note that DSS05 is stuck at level 2, indicating gaps in endpoint security policies, access policies, and event log management in IT incidents. These results highlight the urgency of improvements and enhancements in IT governance in the enterprise sector, especially in the DSS05 subdomain. Closing this gap requires immediate improvements in endpoint security policies, access policies, and event logs in IT incidents so they can be quickly resolved.

Corresponding Author **:**
Rudi Sutomo
Information Systems, Faculty of Engineering and Informatics, Universitas Multimedia Nusantara.
Scientia Garden Jl. Boulevard Gading Serpong, Kab. Tangerang-Banten, 15810.
Email: rudi.sutomo@umn.ac.id

INTRODUCTION

Nowadays, the advancement of technology has touched various fields of human life, ranging from communication technology, transportation, medicine, education, architecture, and construction to business world companies (Oktarina, 2022). Information technology's production, storage, development, delivery, and dissemination are all aspects (Joanda et al., 2021). Information technology governance is essential for managing every business activity. Companies must better manage the strategies and policies of organizational infrastructure and information technology services (Supangat, 2021).

Information technology improves operational activities, provides valuable benefits, and adds value to the company or institution (Romadhon et al., 2018). The application of information technology in a company or organization includes the implementation of IT in the company (Mariatama et al., 2022). IT installation in a business is increasingly considered the "backbone" of the organization's operations. The organization undergoes numerous changes due to the IT adoption (Lee, 2018). IT implementation in the company requires alignment between the IT and business divisions. One way to realize this alignment is the implementation of IT Governance (Riana, 2020).

IT governance implementation (Riana,2020). In the nearby business sector, IT Governance has been implemented in businesses. Private enterprises transmit information to the BUMN scale (Sugiharto, 2021). State-owned enterprises (BUMN) are business entities whose capital ownership comes from the state. BUMN business capital comes from direct capital participation provided by the state (Karim et al., 2020). Implementing IT Governance within the purview of SOEs is governed by the Ministerial Regulation of SOEs No.2 of 2013 concerning Guidelines for the Preparation of Information Technology Management of State-Owned Enterprises. State-owned companies have also thoughtfully implemented how to implement and secure IT implementation within the company (Safitri, 2021). According to paragraph 1 of Article 2, information technology (IT) governance is the basis for the use and growth of SOE information technology (Kementerian et al., 2013). As stated and applicable, the Business Sector must also implement the Permen BUMN. As a BUMN, the Business Sector is also bound by the stipulated Permen BUMN. Therefore, in addition to finalizing IT performance in the company, the Business Sector must also fulfill the stipulated provisions, one of which is by conducting measurements (assessment) in the company's IT implementation.

A business specializing in aviation MRO and offering related industrial services is the Business Sector. They are Indonesia's biggest MRO service provider and have over 70 years of experience. Business Sector currently works with clients in more than 60 different nations. Business Sector has been certified by more than 20 civil aviation authorities as a top-tier MRO, including EASA (Europe), FAA (America), CASA (Australia), and DGCA (Indonesia) (GMF Team, 2023). Considering the broad scope of the Business Sector, the Business Sector needs a mature IT system to improve their services. A sound IT system is necessary because, in addition to improving service performance, IT systems can also improve business strategies. A sound IT system can also be a superior value in market competition in this globalization era (Dharma et al., 2021). It is essential to integrate the IT system development process with the goals and needs of the business. The alignment completed will deliver (display) more maximum value from developing the IT system (Simarmata et al., 2020).

The COBIT 2019 framework offers a feature to gauge an organization's IT maturity level. The level and value of the maturity of the control of IT processes are assessed using the COBIT 2019 framework (Andi et al., 2022). COBIT 2019 has the potential to facilitate the development of effective policies to control information technology in an organization. In addition, its use can also improve the quality and simplify the implementation of organizational processes (Christian et al., 2023).

RESEARCH METHOD

ISACA's rules and regulations carry out the COBIT 2019 framework measurement method (Information et al. Association, 2018). A competence level and gap analysis inside the company are produced due to the measurement done. Quantitative (questionnaire) and qualitative (interviews and literature review) methods were used to collect the data.

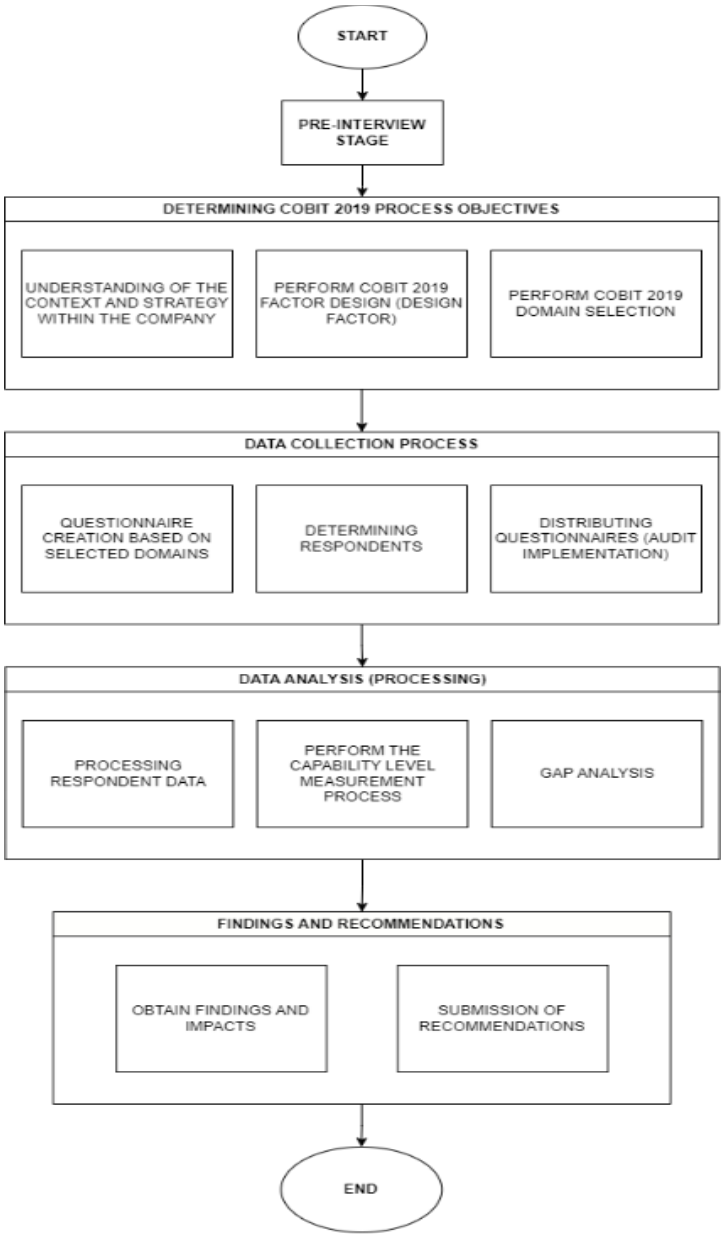

Figure 1. Research Framework

Figure 2 shows the flow of the research framework. Pre-interview with the Business Sector by asking questions about the initial description of the company, as well as conveying the purpose and objectives of the research. The next stage conducts a discussion that discusses understanding the context and strategy of the company, as well as the problems (focus areas) that exist in the company. After the discussion, proceed to the following process, which is the design process in the COBIT 2019 Design Factor. Design considerations can assist businesses in developing governance systems with the stated focus (Information et al. Association, 2018). After carrying out the design process from the Design Factor, it will be found out what COBIT 2019 domains are needed in the research so that these domains can be used to measure the level of IT Security in the company.

After knowing what domains are used in the research, the following process determines the respondents to the questionnaires to be distributed. Selection of respondents using the RACI Chart by the distribution of activities that have been determined in the 2019 COBIT book. Using the RACI Chart, we can quickly determine the level of involvement of each party in each activity (Rohadatul aisy, 2020).

In the Data Analysis (Processing) stage, the activity begins with the collection of questionnaire data that has been distributed, which will then enter the process of measuring the capability level of the questionnaire answers received (Yasin et al., 2020). In the COBIT 2019 framework, researchers use a rating scale to measure capability achievement (Fradinata et al., 2021). From this process, whether there is a gap (GAP) in the company will be found. Gap Analysis is a tool used to evaluate the company's performance gap within internal management management (Kinanti, 2022).

At the Findings and Recommendations stage, it enters the final stage of company research. The process at this stage is to obtain (know) the findings and impacts on the company. The findings obtained come from the stages that have been carried out previously. After finding the findings and their impact, it can proceed to the following process: drawing conclusions in the research and submitting recommendations to the company (I Putu Agus Swastika et al., n.d.).

RESULT AND DISCUSSION

The results and discussion section presents the data analysis findings (not the raw data). Tables and graphs can help in presentation, but they must be supported by explanations that contextualize the study's findings. The discussion continues by comparing the research findings to prior findings, theories, or bodies of knowledge supported by references. Research findings may be in agreement with one another, not in agreement with one another, or even contradict one another.

Pre-Interview Stage

After conducting a pre-interview stage with the Business Sector, there are problems in the IT Security focus area. The results of the pre-interview stage show that the Business Sector has IT Security problems in the company's internal applications that can be accessed online or using the internet. The problem leads to data leaks and hacking on the company's internal applications.

Understanding the Context and Strategy within the Company

After conducting the pre-interview stage, the results obtained are the background of the problems that exist in the company. The outcomes of the pre-interview stage reveal that the Business Sector has IT Security issues with the organization's internal programs that can be accessed online or utilizing the internet. The issue in question results in data breaches and intrusions into the company's internal systems.

Determine the Scope of the Governance System

This stage fills in design factors 1 – 4 to determine the company's scope. Design Factor 1 - Enterprise Strategy, Business Sector focuses on Growth/Acquisition. Business Sector rated the importance of Growth/Acquisition at 5. This shows that the Business Sector focuses on the growth and revenue of the company. Business Sector is concerned with five value enterprise goals, including a portfolio of competitive products and services, compliance with external laws and regulations, a culture of customer-oriented service, optimization of internal business process functionality, and product and business innovation, according to the results of Design Factor 2 (DF-2) analysis. The most significant risk is associated with Design Factor 3 - Risk Profile, IT Cost, and Oversight. Followed by the second rank is IT Operational infrastructure incidents. Then below that, which is still considered a high enough risk, are five other scenarios. Design Factor 4 – IT-Related Issues The Business Sector has 15 IT-related issues considered severe in the 2019 COBIT design toolkit.

Refine the Scope of the Governance System

In order to clarify the scope of the governance system, this stage fills in design criteria 5 through 11. Design Factor 5 – The Thread Landscape Business Sector considers threads (threats) in IT to be at a high level. The percentage of normal levels is at 80%, and the percentage of high levels is at 20%. These findings also conclude that the Business Sector needs different emphasis areas in the Information Security Emphasis Area. Design Factor 6: Compliance Requirement: Business Sector is more prone to high-level regulation, with a percentage value of 78%. The percentage at a high level dominates the low and normal levels, which are at 12% and 10%. Design Factor 7 - Role of IT Business Sector shows that the role of the IT Business Sector tends to be in the strategic classification. These findings demonstrate how crucial it is for the business sector to incorporate IT into developing and managing business operations and corporate services. Its sourcing model is classified as insourced by Design Factor 8 - Sourcing Model for IT, Business Sector. DevOps is the category for its IT implementation according to Design Factor 9 - Implementation Methods, Business Sector. The company uses the DevOps working method for development, implementation, and operations. Design Factor 10 - Technology Adaptation Strategy: The Business Sector is a follower in technology adoption. Instead of being the first to adopt a technology, the business sector adopts it after it has been tried and verified. Enterprise size Design Factor 11 is not included in the 2019 COBIT design tools. The number of employees or employees in the company can be used to determine the size of the enterprise. Official data on the number of employees in the Business Sector amounted to more than 5,000 as of May 2023. From the number of employees in the company it shows that Business Sector is a Large Enterprise.

Summarize the Governance System Design

Three sub-domains were chosen as measurements in the Business Sector. The three sub-domains were chosen because they are related to the chosen writing topic related to IT Security. The three sub-domains include APO12-Managed Risk, APO13-Managed Security, and DSS05-Managed Security Services. In addition to these reasons, the three sub-domains were chosen because they are relevant for measurement, with an expected capability level of level 2 to level 3. The company's requirement (history), undertaking Digital Operation Enchantment, and moving toward enormous digitization in the master plan for the following year strengthened the decision to choose these three sub-domains. Because of this, the business sector needs sophisticated IT security to carry out long-term corporate goals.

Data Collection

In collecting data from the Business Sector to continue the measurement process using the APO12-Managed Risk, APO13-Managed Security, and DSS05-Managed Security sub-domains, a questionnaire was filled out to determine the objective value. The questionnaire was distributed using the Google Form platform and then distributed to respondents.

Determining Audit Respondents Using the RACI Chart

The following Table. 1,2,3 is the RACI Chart of Business Sector respondents on process objectives APO12, APO13, and DSS05 based on COBIT 2019:

Table 1. RACI Chart APO12-Managed Risk

Activities	Manager Innovation & IT Project Management	SM Information & Digital Transformation	Vice President
APO12.01 Collect data.	R	R	C/I
APO12.02 Analyze risk.	-	R	C/I
APO12.03 Maintain a risk profile.	-	R	C/I
APO12.04 Articulate risk.	-	R	C/I
APO12.05 Define a risk management action portfolio.	R	R	C/I
APO12.06 Respond to risk.		R	C/I

It can be seen from table 1. There are three positions in the company that represent job functions on the RACI Chart. These positions include Manager, Senior Manager and Vice

President. For senior managers, they have R (Responsible) and A (Accountability) in each management practice in the APO12 sub-domain. Meanwhile, for managers, there are only two Rs in the APO12 sub-domain. Then for the vice president there are consulted (C) and informed (I) in the 2019 COBIT measurement process.

Table 2. RACI Chart APO13- Managed Security

Activities	Manager Innovation & IT Project Management	SM Information & Digital Transformation	Vice President
APO13.01 Establish and maintain an information security management system (ISMS).	R	R	C/I
APO13.02 Define and manage an information security and privacy risk treatment plan.	R	R	C/I
APO13.03 Monitor and review the information security management system (ISMS).	R	R	C/I

In Table 2, it can be seen that in the APO13—Managed Security sub-domain there are three management practices where the Manager and Senior Manager are both responsible (R). then in the third position (Vice President) has the role of informed (I) and also consulted (C).

Table 3. RACI Chart DSS05- Managed Security Services

Activities	Manager Innovation & IT Project Management	SM Information & Digital Transformation	Vice President
DSS05.01 Protect against malicious software.	R	R	C/I
DSS05.02 Manage network and connectivity security.	R	R	C/I
DSS05.03 Manage endpoint security.	R	R	C/I
DSS05.04 Manage user identity and logical access.	R	A	C/I
DSS05.05 Manage physical access to I&T assets.	R	A	C/I
DSS05.06 Manage sensitive documents and output devices.	R	A	C/I
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	R	A	C/I

Shown in Table 3. Manager responsible (R) in the seven management practices. Meanwhile, with Senior Managers, they are only responsible and accountable in management practices 1 – 3. Then for Vice Managers, they play a role in consulting and informing in all management practices in DSS05—Managed Security.

Activity Analysis and Capability Level

Based on the answers to the questionnaire from SM Information & Digital Transformation and Manager of Innovation & IT Project Management at Business Sector, the following calculation results have been obtained, shown in Table 4.

Table 4. RACI Chart APO13- Managed Security

Result	Average	Expected	Actual
APO12-Managed Risk	60%	2	2
APO13- Managed Security	81,78%	2	2
DSS05- Managed Security Services	77,80%	3	2

The outcomes of the APO12-Managed Risk sub-domain process are said to halt at level 2 capability level with a value of 60%, according to the scoring results when taking measurements. With this % value, it is clear that the business sector has attained the Largely Achieved (L) grade

at level 2 competence level. The next sub-domain is APO13-Managed Security, focusing on the information security management system. From the measurement and scoring results, it stops at level two with a value of 81.78%. It can be concluded that with the significant percentage value, the Business Sector reached level 2 capability level with the Largely Achieved (L) ranking.

The third sub-domain, DSS05-Managed Security Services, focuses on maintaining information security by policies within the company. From the measurement results, according to the value (score), it must stop at level 2 with a percentage of 77.80%. It can be concluded that the Business Sector can only reach level 2 capability because the percentage value is less than 85%. This makes the Business Sector unable to continue to the next level even though the expected level of capability is at level 3.

GAP Analyst

After all sub-domains have been calculated, the next step is to compare the design toolkit's target level (expected level) with the measurement results. Gap analysis can make it easier to describe the comparison between the target level and the expected level. Calculation results (actual level). Table 5 contains the gap analyst calculation's findings.

Table 5. GAP Analyst Result

Objective	Expected Level	Actual Level	Gap
APO12-Managed Risk	2	2	0
APO13- Managed Security	2	2	0
DSS05- Managed Security Services	3	2	1

DSS05-Managed Security Services expected the highest level of capability among the three other sub-domains, which is level 3. This shows that the DSS05-Managed Security Services sub-domain requires further measurement to level 3 if the capability at level 2 has been met. However, in reality, Business Sector is currently at level 2 capability because the level 2 measurement results are not met for research to the next level. For this reason, improvement recommendations are needed so that the Business Sector can be at a better level of capability in the DSS05-Managed Security Services sub-domain.

Findings and Recommendations from IT Governance Capability Measurement Results

After measuring the capability level in the Business Sector with the selected sub-domains, findings and impacts were found from the activities measured. Findings are taken from activities whose values do not meet the average rating scale's requirements. A list of findings is shown in Table 6.

Table 6. Findings

Objective	Findings
APO12-Managed Risk	IT risk analysis is not integrated or managed separately from enterprise risk management. Identifying support staff, applications, infrastructure, facilities, crucial manual records, vendors, suppliers, and outsourcers is not covered in any extensive (complete) documentation about IT service management.
APO13-Managed Security	Lack of comprehensive and periodic awareness of the information security management system to the entire company entity, which is a direct part of the SMKI element.
DSS05-Managed Security Services	No device lockdown mechanism yet The internal network within the Business Sector is managed, but when the endpoint has used an external network (outside the Business Sector), there is no company network management. When in the internal network, the bandwidth management tool used is not available

There are findings and impacts in APO12-Managed Risk. The first finding and impact is a combination of three management practices and four activities. This happens because the four activities discuss the same core of IT risk. Then, the second finding and impact comes from APO12.03, which leans towards documentation. Then, there is one finding and impact the Business Sector has confirmed in APO13-Managed Security regarding SMKI. Finally, in DSS05,

two existing findings regarding the company's endpoint devices exist. However, the second finding has two split findings, namely, between internal network management and bandwidth management tools within the company.

After obtaining the findings and the impact of the findings resulting from the findings, some recommendations can be given to the company. The following in Table 7 is a list of improvement suggestions for the sub-domains.

Table 7. Improvement Recommendations

Objective	Activity	PIC
APO12-Managed Risk	1) Manage the IT risk register with enterprise risk management as one. 2) Implement a detailed documentation system that can be accessed by company personnel.	IT Governance & Risk Officer and SM Innovation & Digital Transformation
APO13-Managed Security	Provide knowledge of the information security management system to all company entities.	IT Security Officer
DSS05-Managed Security Services	1) Implement a device lockdown mechanism to avoid potential data misuse when endpoint devices are outside of Business Sector's control. 2) Restrict access when using external networks on endpoint devices to prevent external attacks. 3) Periodically manage the bandwidth management tools used so that network traffic within the company can be used without interruption.	IT Service Delivery and IT Network Analyst

The first recommendation is a combination of several management practices and activities in APO12. This happens because in management practice and these activities have the same root problems (findings). Then the second recommendation for improvement is aimed at APO12.03 activity 1. recommendations to improve several activities in APO13.01. recommendations given regarding the information security management system. The company accepted all improvement recommendations, but the device lockdown mechanism and restricting device access still need to be considered internally.

Level Up Recommendation

Level improvement recommendations are given so that the Business Sector can meet the expected capability level according to the results in the design factor. Improvement recommendations are also needed so that the Business Sector can overcome the level gap in their IT governance process. Providing recommendations for level improvement in the Business Sector is in the DSS05-Managed Security Service sub-domain process because it has not met the expected level of capability. The following in Table 8 is a level improvement recommendation for sub-domain DSS05

Table 8. Improvement Recommendations

Sub-Process	Activity	PIC
DSS05.03	1) Implement a device lockdown mechanism to avoid potential data misuse when endpoint devices are out of the Business Sector's control. 2) Apply traffic filtering to endpoint devices. 3) Maintain the integrity of the system, which means ensuring that information and systems are secure to perform functions free from manipulation interference, intentional or unintentional, following the company's Security Policies. 4) Provide (reinforce) physical protection to endpoint devices. Implement a detailed documentation system that is accessible to company personnel.	SM IT Service Delivery

Sub-Process	Activity	PIC
DSS05.05	1) Impose strict supervision requirements for guests on the IT site.	IT Service Delivery
DSS05.06	1) Establish (enhance) processes to control the entry, use, deletion, and disposal of sensitive documents and output devices when documents enter, are used inside, or are used outside the organization. 2) Make sure that cryptographic controls protect the electronic storage of sensitive information.	IT Security Officer
DSS05.07	1) Define and communicate risk scenarios to quickly recognize and understand the likelihood and impact of risks that occur. 2) Review event logs regularly to understand the potential for incidents to occur. 3) When monitoring and spotting potential events, promptly create security-related incident tickets.	IT Security Officer

The recommendations given refer to the 2019 ISACA COBIT book. In the 2019 COBIT book, an output contains a big picture of improvements (evaluation) in sub-domain DSS05.03. The results indicate that the Business Sector needs to review (better) its access rights regulations, endpoint device security policies, and security event logs (IT incidents).

CONCLUSION AND SUGGESTION

Conclusion

Following the completion of the measurement of information technology governance in the Business Sector using the 2019 COBIT framework, it can be said that the results of the calculation of the capability level value in the APO12-Managed Risk sub-domain reach level 2 with an average value of 60% so that it is at the fully achieved level. In addition, the APO13-Managed Security sub-domain achieves level 2 capability with an average result of 81.78%, indicating that this sub-domain has achieved the Largely Achieved class at level 2. DSS05-Managed Security Service is the final sub-domain in the measurement process. The measurement process's findings reveal that DSS05 averages 77.80% at level 2. This indicates that DSS05 cannot proceed to the level 3 process since it only achieves Largely Achieved even though the level at which it should be is level 3. Reviewing the results of measuring the competence of the processes in numerous sub-domains shows that the three sub-domains are still at the Largely Achieved level, below 85%. When traced further, several findings in the processes in each sub-domain occur. While in the DSS05-Managed Security Service sub-domain, there is a gap because DSS05 cannot reach the expected level, namely level 3. Based on the average sub-domain measurement results, there are recommendations for improvement and increasing the level of processes measured in the Business Sector. To close any gaps, suggestions are made. Reviewing (improving) endpoint device security policies, access rights policies, and security event logs is necessary for critical suggestions in the business sector-level improvement recommendations.

Suggestion

1) Identify improvement recommendations from existing company findings and track their success in implementation.
2) Measuring processes in other domains or sub-domains because there are a total of 24 sub-domains that are relevant for measurement in the Business Sector.

ACKNOWLEDGEMENT

Thank you to Universitas Multimedia Nusantara, especially the Faculty of Engineering & Informatics, for assisting and offering direction with the planning and writing of this journal paper. Also, thank you to the business for permitting measurements using COBIT 2019.

REFERENCES

Andi Nurul Istiyana, S. S. T. M. A. (2022). *Buku Ajar Audit Sistem Informasi*. Nas Media Pustaka. https://books.google.co.id/books?id=o9-SEAAAQBAJ

Christian, T. D., Nama, G. F., Sulistiono, W. E., & Muhammad, M. A. (2023). Analisis Tata Kelola Teknologi Informasi Bedasarkan COBIT 5 Fokus *Subdomain Deliver, Service*, and *Support0*1 (DSS01)(Studi Kasus: PT Cerita Teknologi Indonesia). *Jurnal Informatika Dan Teknik Elektro Terapan*, *11*(1). https://doi.org/10.23960/jitet.v11i1.2825

Dharma, I. G. M. S., Sasmita, G. M. A., & Putra, I. M. S. (2021). Evaluasi dan Implementasi Tata Kelola TI Menggunakan COBIT 2019 (Studi Kasus pada Dinas Kependudukan dan Pencatatan Sipil Kabupaten Tabanan). *Jurnal Ilmiah Teknologi Dan Komputer*, *2*(2), 354–365.

Fradinata, M. R., Putra, I. G. J. E., & Wijaya, I. N. Y. A. (2021). Evaluasi Tata Kelola TI Menggunakan Framework COBIT 5 Studi Kasus STMIK Primakara. *KARMAPATI (Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika)*, *10*(1), 68–77.

GMF Team. (2023). *Onboarding Presentation*. https://www.gmf-aeroasia.co.id/

I Putu Agus Swastika, M. K., I Gusti Lanang Agung Raditya Putra, S. P. M. T., Pramesta, A., OFFSET, C. V. A., & primakara, S. (n.d.). *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*. Penerbit Andi. https://books.google.co.id/books?id=_iU3DgAAQBAJ

Information Systems Audit and Control Association. (2018). *COBIT® 2019 Framework : introduction and methodology*.

Joanda Kaunang, F., & Karim, A. (2021). *Konsep Teknologi Informasi* . Yayasan Kita Menulis. https://books.google.co.id/books?hl=en&lr=&id=cIUeEAAAQBAJ&oi=fnd&pg=PA4&dq=Teknologi+Informasi&ots=hKTeYLYRaN&sig=lbupph62O1uiMyH1Tn9GRBLiB1I&redir_esc=y#v=onepage&q=Teknologi%20Informasi&f=false

Karim, A., Bangun, B., Purnama, I., Harahap, S. Z., Irmayani, D., Nasution, M., Haris, M., & Munthe, I. R. (2020). *Pengantar teknologi informasi*. Yayasan Labuhanbatu Berbagi Gemilang.

Kementerian Badan Usaha Milik Negara. (2013). Peraturan Menteri Badan Usaha Milik Negara tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara. *Peraturan Menteri Badan Usaha Milik Negara*, 2–2.

Kinanti, T. A. (2022). *pengukuran kinerja pelayanan disamsat kota banjar menggunakan cobit 2019 dan metode sevqual*.

Lee, M. V. W. (2018). *Pengukuran Tingkat Kematangan Service Operation Departemen TI UMN Menggunakan Kerangka Kerja ITIL 2011*.

Mariatama, A. A., Atrinawati, L. H., Gilvy, M., Putra, L., Informasi, S., Kalimantan, T., Sei, J., Km, W., Karang, K., Kecamatan, J., & Utara, B. (2022). *Perancangan Tata Kelola Teknologi Informasi Dengan Menggunakan Framework COBIT 2019 Pada PT JWT Global Logistics Indonesia* (Vol. 5, Issue 1).

Oktarina, T. (2022). Tata Kelola Teknologi Informasi Dengan COBIT. *Tata Kelola Teknologi Informasi Dengan COBIT*.

Riana, E. (2020). Implementasi Cloud Computing Technology dan Dampaknya Terhadap Kelangsungan Bisnis Perusahaan Dengan Menggunakan Metode Agile dan Studi Literatur. *JURIKOM (Jurnal Riset Komputer)*, *7*(3), 439–449.

Rohadatul Aisy, S. (2020). *Audit Teknologi Informasi Dengan Framework COBIT 4.1 Untuk Manajemen Risiko Pada PUSTIPD UIN Raden Fatah Palembang*.

Romadhon, A., Teja Sukmana, H., & Ummi Masruroh, S. (2018). *Konferensi Nasional Sistem Informasi 2018 STMIK Atma Luhur Pangkalpinang*.

Safitri, L. (2021). Analisis Efektivitas Aplikasi Cek DJP Online Pajak dan Laporan SPT Tahunan E-filling Menggunakan Framework COBIT 5 Domain EDM (Evaluate, Direct, and Monitor) pada KPP Pratama Tanjungpinang. *Bangkit Indonesia*, *X*(02).

Simarmata, J., Romindo, R., Putra, S. H., Prasetio, A., Siregar, M. N. H., Ardiana, D. P. Y., Chamidah, D., Purba, B., & Jamaludin, J. (2020). *Teknologi Informasi dan Sistem Informasi Manajemen*. Yayasan Kita Menulis.

Sugiharto, A. J. (2021). Kerugian Badan Usaha Milik Negara (BUMN) Sebagai Kerugian Keuangan Negara. *Jurnal Education And Development*, *9*(1), 158.

Supangat, R. (2021). *Analisis Tingkat Kematangan dan Perancangan Peningkatan Layanan Sistem Informasi Rektorat Universitas 17 Agustus 1945 Surabaya*.

Yasin, M., Arman, A. A., Edward, I. J. M., & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001: 2013 (Case et al.). *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, pp. 1–5.