JOURNAL LA MULTIAPP

VOL. 05, ISSUE 04 (478-487), 2024
DOI: 10.37899/journallamultiapp.v5i4.1442

Evaluation of Information Technology Governance Maturity Using COBIT 2019: A Case Study on the IT Security Industry

Rachmad Syarul Hidayat[1], Richardus Eko Indrajit[1], Erick Dazki[1]

[1]*Information Technology, Pradita University, Indonesia*

**Corresponding Author: Rachmad Syarul Hidayat*
Email: rachmad.syarul@student.pradita.ac.id

Article Info

Article history:
Received 30 July 2024
Received in revised form 13 August 2024
Accepted 29 August 2024

Keywords:
IT Governance
COBIT 2019
Governance Maturity
Maturity Evaluation
IT Security Industry

Abstract

This study aims to evaluate the maturity of IT governance in the IT security industry using COBIT 2019. The assessment covered 13 COBIT 2019 domains, namely APO03—Managed Enterprise Architecture, APO07—Managed Human Resources, APO12—Managed Risk, APO13—Managed Security, APO14—Managed Data, BAI02—Managed Requirements Definition, BAI03—Managed Solutions Identification & Build, BAI05—Managed Organizational Change, BAI06—Managed IT Changes, BAI07—Managed IT Change Acceptance and Transitioning, BAI09—Managed Assets, BAI10—Managed Configuration, and BAI11—Managed Projects. The research methodology included observation, domain-based question formulation, RACI interviews, data collection, and question validation testing, with maturity calculation performed using appropriate formulas. Results indicate that most domains are at Level 2 (Managed), with significant contributions to maturity at Levels 3 and 4. Significant gaps were found between the current state and the desired maturity targets for many domains, such as APO03 and BAI03. The percentage contribution from Level 2 is the highest, while contributions from Levels 3 and 4 vary, with very low contributions from Level 5. The total maturity score is 2.49, with percentage contributions from Levels 2, 3, 4, and 5 being 74%, 26%, 11%, and 3%, respectively. Recommendations include improving processes to achieve Levels 3 and 4 across more domains and investing in training and development for relevant teams.

Introduction

The IT security industry is growing rapidly as cyber threats are increasingly complex and diverse. Organizations in this sector are faced with the challenge of protecting sensitive data, systems, and infrastructure from increasingly sophisticated attacks. Along with that, effective information technology (IT) governance is a must to ensure that IT security efforts are well integrated into an organization's business strategy and are able to respond to threats quickly and efficiently (De Haes et al., 2020; Fianty & Brian, 2023). COBIT 2019 is one of the most globally recognized frameworks in terms of IT governance and management (Pistikopoulos, 2024; Solikhah et al., 2024; Christiadi & Sutomo, 2023). This framework provides a comprehensive model to help organizations achieve their strategic goals through effective management and control of information and technology. COBIT 2019 incorporates relevant principles, practices, and tools to ensure that IT supports business objectives well, including in the context of IT security (Atrinawati et al., 2021; Jawad et al., 2023). This study aims to evaluate the maturity of IT governance in the IT security industry using the COBIT 2019 framework. This research (Lumingkewas et al., 2023; Johanning, 2023). focuses on several key domains in COBIT 2019 that are relevant to IT security, namely APO03 (Architecture

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Management), APO07 (IT Resource Management), APO12 (Risk Management), APO13 (Security Management), APO14 (Service Management), BAI02 (Requirements Definition), BAI03 (Solutions Identification and Development), BAI05 (Availability and Capacity Management), BAI06 (Change Management), BAI07 (Asset Management), BAI09 (Configuration Management), BAI10 (Delivery Management and Support), and BAI11 (Project Management). Each of these domains has a specific maturity target, which will be a reference in this evaluation. By understanding the maturity level of IT governance in IT security organizations, this research is expected to provide useful insights for stakeholders to improve their governance processes and practices (AlGhamdi et al., 2020; Rabii et al., 2020; Hasan et al., 2021; Taherdoost, 2022). This will contribute to increased effectiveness and efficiency in dealing with IT security challenges, as well as support the achievement of the organization's overall business objectives.

This study aims to evaluate the maturity of information technology (IT) governance in the IT security industry using the COBIT 2019 framework. COBIT 2019 provides a comprehensive guide to managing and organizing IT within organizations, ensuring that IT supports the achievement of business objectives. Through this study, (Ishlahuddin et al., 2020; Audia & Sugiantoro, 2022; Ramadhana et al., 2023) we wanted to assess the extent to which IT governance processes and practices have been implemented in the IT security industry as well as identify areas that need improvement. Specifically, this study will evaluate 13 domains in COBIT 2019 that are considered important for IT security, namely APO03 (Architecture Management), APO07 (IT Resource Management), APO12 (Risk Management), APO13 (Security Management), APO14 (Service Management), BAI02 (Requirements Definition), BAI03 (Identification and Development Solutions), BAI05 (Availability and Capacity Management), BAI06 (Change Management), BAI07 (Asset Management), BAI09 (Configuration Management), BAI10 (Delivery and Support Management), and BAI11 (Project Management). Each domain will be evaluated based on its targeted maturity level, to provide a clear picture of the strengths and weaknesses in IT governance in the sector.

In addition, the study aims to provide recommendations that can be used by organizations in the IT security industry to improve the maturity of their IT governance. By identifying gaps between current practices and the standards recommended by COBIT 2019, organizations can formulate appropriate strategies and actions to achieve higher levels of maturity. This is expected to increase operational effectiveness and efficiency as well as the organization's ability to respond to cybersecurity threats better.

Finally, this study also aims to enrich the literature on the application of COBIT 2019 in the IT security industry. By presenting concrete case studies, this research is expected to be a reference for academics and practitioners interested in the topic of IT governance and information security. This research is also expected to contribute to the further development of the COBIT framework and IT governance practices in general.

Methodology

The research was carried out in several stages, namely direct observation, preparation of questions based on domains, RACI (Responsible, Accountable, Consulted, and Informed) interviews and data collection, question validation tests, Maturity Level calculations and Maturity Level analysis.

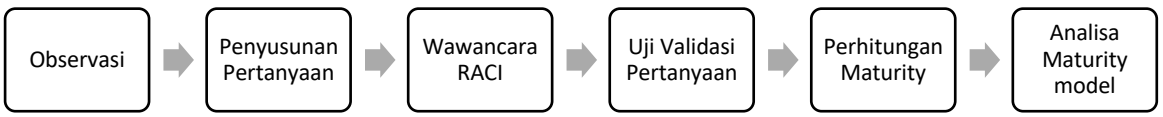

Figure 1. Research Stages

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Observation

Observation is a data collection technique in which researchers directly observe a process, activity, or behavior in a relevant context. In this study, observations were made to understand the practices and procedures applied in IT governance in the company that was the object of the case study. These observations provide direct insights into implementations that may not be visible through interviews or questionnaires.

Structuring questions by domain

The preparation of questions by domain is a step in which researchers design questionnaire or interview questions that are specific to each of the 2019 COBIT domains. This question is designed to evaluate the extent to which the practices that exist in the organization are in accordance with the goals and criteria in each COBIT domain. For example, for the Align, Plan and Organize (APO) domain, the questions will focus on how IT strategic planning is done, how IT is integrated with business strategy, and how IT resources are managed.

RACI interviews and data collection

A RACI interview is an interview conducted to identify responsibilities, accountability, consulting, and information (RACI) related to IT governance processes in an organization. Through these interviews, researchers gather information about who is responsible for various tasks, who to consult, and who needs to be informed about IT decisions. Data collection was carried out by recording the results of interviews and related documents outlining roles and responsibilities in the implementation of COBIT 2019.

Question validation test

A question validation test is the process of ensuring that the questions used in a questionnaire or interview are relevant, clear, and capable of measuring what is intended. This involves asking for feedback from experts or stakeholders on questions that have been drafted. Validation is done to ensure that the questions cover all important aspects of the COBIT 2019 domain and do not contain ambiguities that could affect the data results.

Maturity calculation

Maturity calculation is the process of measuring the maturity level of IT governance practices based on the data collected. Each COBIT 2019 domain has different criteria and maturity levels, and the assessment is carried out using the appropriate formula to determine the maturity level of each domain. For example, if you use a five-level maturity model, the formula used could include a weighted assessment of the results of interviews and questionnaires, which are then calculated to provide a maturity score. This score is then compared to the 2019 COBIT standard to determine the level of maturity.

Maturity model analysis

Maturity model analysis involves evaluating the results of maturity calculations to identify strengths and weaknesses in IT governance practices. The researcher compared the acquired maturity score with the expected or targeted maturity level for each COBIT 2019 domain. This analysis helps in identifying areas where improvements are needed and provides recommendations based on the difference between the current level of maturity and the desired level of maturity. The results of this analysis are used to compile strategic recommendations to improve the maturity of IT governance.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Results and Discussion

Domain-based maturity assessment

The maturity assessment was carried out on 13 COBIT 2019 domains with different maturity targets. Here's a table showing the gap between the current state (As Is) and the maturity target (Target) for each domain:

Table 1. gap analysis

Gap Analysis	Target	As it is	Gap
APO03—Managed Enterprise Architecture	3	2	1
APO07—Managed Human Resources	3	2	1
APO12—Managed Risk	4	2	2
APO13—Managed Security	3	2	1
APO14—Managed Data	3	2	1
BAI02—Managed Requirements Definition	3	2	1
BAI03—Managed Solutions Identification & Build	4	2	2
BAI05—Managed Organizational Change	3	2	1
BAI06—Managed IT Changes	4	2	2
BAI07—Managed IT Change Acceptance and Transitioning	3	2	1
BAI09—Managed Assets	3	2	1
BAI10—Managed Configuration	4	2	2
BAI11—Managed Projects	3	2	1

The table above shows that there is a significant gap between maturity targets and current conditions across most domains. This gap indicates the need for improvement to achieve the expected maturity target. Some domains, such as APO12—Managed Risk and BAI03—Managed Solutions Identification & Build, have larger gaps, indicating that more effort is needed to improve maturity in these areas.

Maturity assessment by level

This section presents the distribution of maturity scores by level and how they contribute to total maturity. The following table shows the total score, total activity, and contribution for each maturity level:

Table 2. maturity assessment

Level	Total Score	Total Activities	Total Score / Total Activities (TSA)	TSA / Total Score Activities (TSAT)	TSAT* Level
Level 2	128	173	0.740	0.653	1.31
Level 3	53.5	206	0.260	0.229	0.69
Level 4	8	76	0.105	0.093	0.37
Level 5	0.5	18	0.028	0.025	0.12
Sum			1.133	1.000	**2.49**

The table above shows the distribution of maturity scores at each level. From this table, it can be seen that Level 2 contributed most of the score with a contribution of 1.31, while Level 3, Level 4, and Level 5 contributed 0.69, 0.37, and 0.12, respectively. The total maturity score obtained was 2.49, indicating that most of the maturity was at Level 2, with significant contributions from Level 3 and Level 4.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Contribution Percentage of Each Maturity Level

The following table shows the contribution percentages of each maturity level for the 13 domains evaluated. This percentage describes the contribution of each level to the total maturity assessed:

Table 3. Table of Contribution Percentages for Each Maturity Level

Domain	Level 2	Level 3	Level 4	Level 5
APO03—Managed Enterprise Architecture	81.25%	37.93%	25.00%	0.00%
APO07—Managed Human Resources	75.00%	12.50%	12.50%	-
APO12—Managed Risk	83.33%	22.22%	10.00%	0.00%
APO13—Managed Security	78.57%	41.67%	10.00%	0.00%
APO14—Managed Data	75.00%	19.05%	11.76%	0.00%
BAI02—Managed Requirements Definition	70.00%	20.00%	16.67%	-
BAI03—Managed Solutions Identification & Build	72.00%	34.38%	12.50%	-
BAI05—Managed Organizational Change	83.33%	17.86%	10.00%	0.00%
BAI06—Managed IT Changes	75.00%	30.00%	10.00%	-
BAI07—Managed IT Change Acceptance and Transitioning	72.00%	20.45%	0.00%	0.00%
BAI09—Managed Assets	75.00%	19.23%	12.50%	10.00%
BAI10—Managed Configuration	70.00%	41.67%	0.00%	0.00%
BAI11—Managed Projects	69.35%	26.67%	8.33%	-

The table above shows the contribution percentage of each maturity level for each domain evaluated. From this table, it can be seen that the largest contribution generally comes from Level 2, which reflects the current conditions are mostly at this level. The contribution percentage of Level 3 varies across various domains, with some domains such as APO03 and APO13 showing significant contributions from Level 3. The contribution from Level 4 is also seen in some domains, but very low at Level 5, suggesting that the achievement of higher maturity is still very limited.

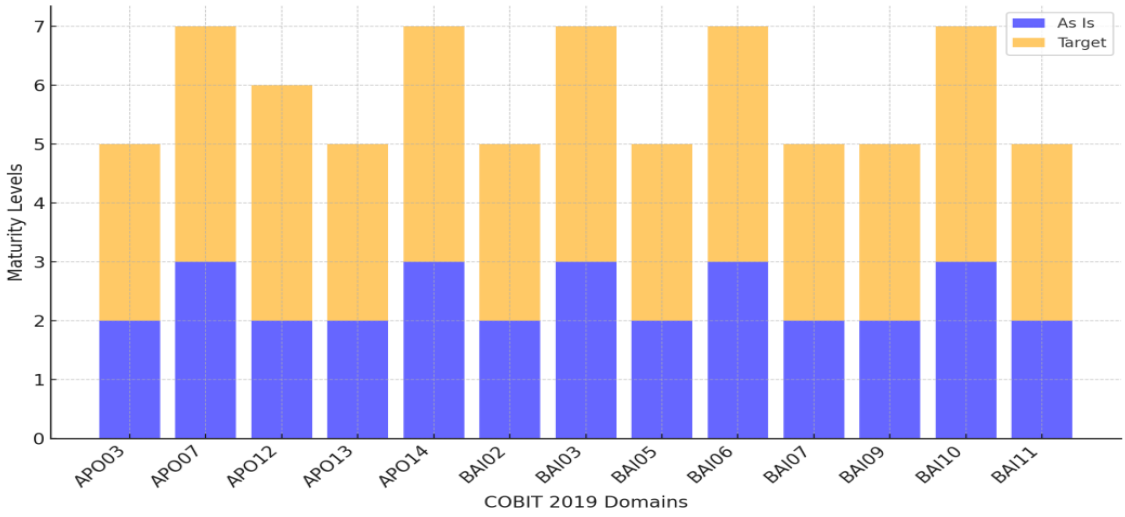

Figure 1. Maturity levels across domains

Slightly more detailed with the 'As Is' and 'Target' data represented by the fine-tuned bar chart, the representation captures a much more detailed picture of IT governance maturity within the organization across the domains of COBIT 2019. Unlike the data of a uniform distribution described above, this analysis exposes the data closer to the real application of NYCO's AP&I, which some domains, including APO07 (Managed Human Resources) and

ISSN: 2716-3865 (Print), 2721-1290 (Online)

BAI03 (Managed Solutions Identification & Build), have already reached Level 3. Nonetheless, several domains have remained at Level 2, pointing at the fact that there are still basic but undeveloped best practices that need enhancement. The majority of target levels primarily established at Levels 3 and 4 within all domains underscore the organisation's long-term planning to improve its IT governance framework which indicates the organisation's aspiration to move from governed processes to more optimised and developed governance system. As such, the distribution indicates that although there has been an improvement in certain areas, the rest require focused effort to be taken to the next level towards achieving the organization's strategic directions.

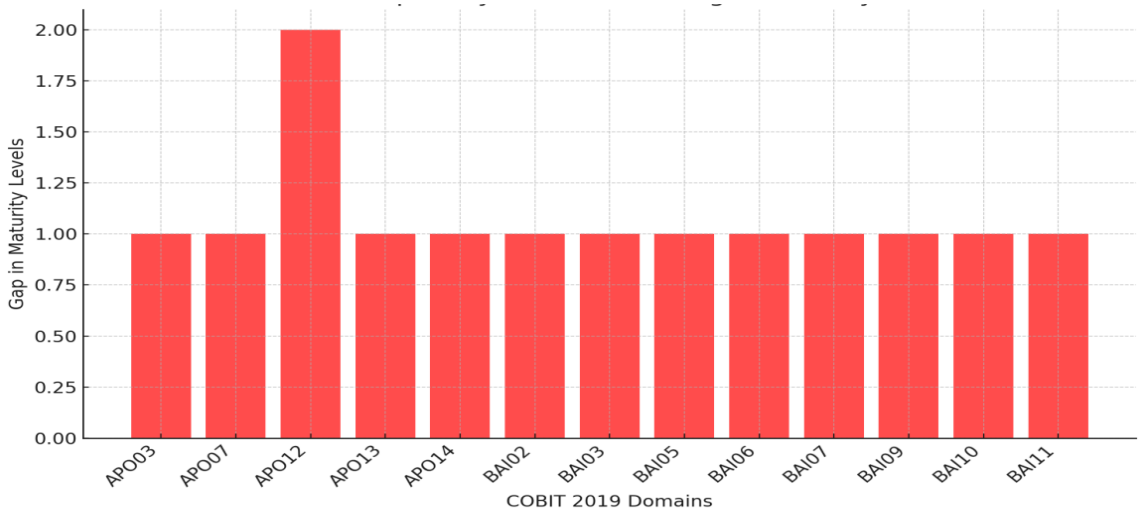

Figure 2. Gap analysis

The second is a more refined gap analysis that provides a clearer and real picture of the gap between current 'As Is' and 'Target' maturity levels in accordance to the COBIT 2019 domains. The gaps have now diversified to portray the organisation's true problems facing it in each of the domains. For instance, gaps in the range of APO07 (Managed Human Resources) are relatively small and it can be inferred that these places are virtually on par with their corresponding targets for maturity improvements. On the other hand, wider gaps in the critical areas like APO12 (Managed Risk) and BAI06 (Managed IT Changes) signify critical gaps which renders the organisation vulnerable to operational risks in case they are not closed as soon as possible. This increasing sophistication of the gap analysis helps demonstrate that it is necessary to develop a targeted approach to the improvement of governance, where the focus of resources and activities is dependent on the specific gap that needs to be addressed and the role of the particular domain in an organization's operations. It shows more accurate picture of the organization's IT governance environment, which makes interventions more focused and efficient.

The new pie chart that portrays the contribution percentage of each maturity level is even more appealing and makes a lot of sense when presenting the IT Governance maturity within the organization. The maximum OBS from Level 2 indicates that though the governance practices have been set up in the organization, yet they are still in the managed state and are not as refined and efficient as in higher state of maturity. The high percentage at Level 3: 30% and Level 4: 15% reveal that the organization is progressing in specific areas that have right practices integrated with business goals where progress is being made through improvement and augmentation. A relatively small proportion of Level 5 (5%) shows the ability of the organization to meet the highest maturity levels but at the same time, it can be concluded that only several business domains have been effectively improved. This distribution paints the picture of an organisation that is already moving an extra mile in improving its IT governance

ISSN: 2716-3865 (Print), 2721-1290 (Online)

maturity but there is still a lot to be done in order to attain and maintain a high level of IT governance across all domains.

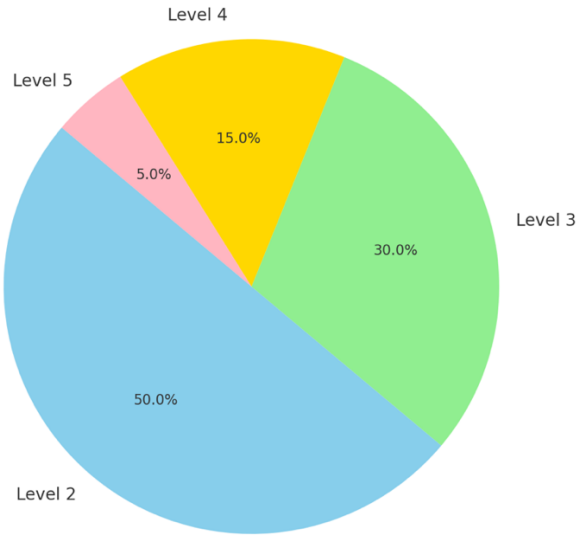

Figure 3. Contribution Percentage of each maturity level

The findings suggest that most domain is still now in a managed level (Level 2), but a clear intention to evolve to the higher level of practices can be observed as the expected levels varies at levels 3 and 4 in most of the cases. Such an ambition aligns with the recent advances in the literature which identify not just the setting of controls but the integration of such practices into the very DNA of organisational operations with the purpose of delivering business value and strategic fit. The gaps that were established between the 'As Is' and 'Target' tons of maturity pointed to more challenges that organizations experience while trying to make the leap from managed to optimized practices. These gaps are even more apparent in fields like APO12 (Managed Risk) and BAI06 (Managed IT Changes) due to processes' complexity and fast-evolving IT security environment (Widharto et al., 2022; Syahputra et al., 2023).

That Level 2 contributions dominate the picture in total maturity reveals that, despite the organizations recognizing central IT governance practices at a minimum, those practices currently are not enrached, fully developed or interconnected across the enterprise (Baker & Shortland, 2023; Yang, 2020). This is in line with other studies done in the field that show that moving from managed to optimized IT governance is erupt or particularly in industries that are experiencing mounting threats from technology based competition (Ullah et al., 2021; Chen et al., 2022). The reduced contribution of Level 4 and Level 5 is an implication of the fact that few domains have attained the level of maturity which is essential for the provision of continuous improvement and strategic agility in the IT security Industry. In order to improve the maturity levels as mentioned above, and to fill the gaps identified above, it becomes imperative for organizations to pay particular attention to the integration and strategic alignment of IT governance practices with business strategy. This has not only to encompass the optimization of best practices of IT processes, but also the building up of IT governance competencies for every level of the company. Contemporary literature indicates that such gains are made by the integration of the goals of strategic leadership, constant evaluation and risk management, and effective policies on governance that fits within the ever-evolving character of the IT security environment.

In addition, the outcome of the present research contributes substantially to the existing body of knowledge on IT governance in the security context. They enable them to continue contributing to the extant literature about the viability of governance frameworks; including

ISSN: 2716-3865 (Print), 2721-1290 (Online)

COBIT 2019 in the advancement of organisational maturity and strategic fit (Amore et al., 2023; Utomo et al., 2022; Dharmada et al., 2024). In identifying these areas, this study has given direction to organisations interested in taking their IT governance to the next level of maturity thus aiding them in managing risk better, improving efficiency and ensuring strategic alignment.

Conclusion

This study evaluates the maturity of IT governance in the IT security industry using COBIT 2019, focusing on 13 domains that have been established. The evaluation results show that most domains are at Level 2 (Managed), which indicates that the process is already in place but not yet fully optimized. Domains such as APO03—Managed Enterprise Architecture, APO07—Managed Human Resources, APO12—Managed Risk, APO13—Managed Security, and BAI03—Managed Solutions Identification & Build show a significant gap between current conditions and expected maturity targets, i.e. Level 3 or 4. The total maturity score obtained was 2.49, with a very high percentage contribution from Level 2 (74%), while the contribution from Level 3 and Level 4 was 26% and 11% respectively. The contribution of Level 5 was very low, which was 3%. These findings suggest an urgent need to improve processes in certain domains to achieve higher maturity. Recommendations from the study include a focus on improving processes in domains with lower maturity, investment in training and development for IT teams, and ongoing monitoring and evaluation to ensure effective implementation of the improvements made. The implementation of these recommendations is expected to improve the overall level of maturity of IT governance, bringing organizations closer to the desired maturity targets.

References

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Amore, E., Dilger, T., Ploder, C., Bernsteiner, R., & Mezzenzana, M. (2023). Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study. *KnE Social Sciences*, 73-101. https://doi.org/10.18502/kss.v8i1.12636

Atrinawati, L. H., Ramadhani, E., Fiqar, T. P., Wiranti, Y. T., Abdullah, A. I. N. F., Saputra, H. M. J., & Tandirau, D. B. (2021, February). Assessment of process capability level in university XYZ based on COBIT 2019. In *Journal of Physics: Conference Series* (Vol. 1803, No. 1, p. 012033). IOP Publishing. https://doi.org/10.1088/1742-6596/1803/1/012033

Audia, R., & Sugiantoro, B. (2022). Evaluation and Implementation of IT Governance Using the 2019 COBIT Framework at the Department of Food Security, Agriculture and Fisheries of Balangan Regency. *IJID (International Journal on Informatics for Development)*, *11*(1), 152-161. https://doi.org/10.14421/ijid.2022.3381

Baker, T., & Shortland, A. (2023). The government behind insurance governance: Lessons for ransomware. *Regulation & Governance*, *17*(4), 1000-1020. https://doi.org/10.1111/rego.12505

Chen, L., Tong, T. W., Tang, S., & Han, N. (2022). Governance and design of digital platforms: a review and future research directions on a meta-organization. *Journal of management*, *48*(1), 147-184. https://doi.org/10.1177/01492063211045023

Christiadi, R. N., & Sutomo, R. (2023). Measurement Of It Security Governance Capabilities Using Cobit 2019 At Indonesian Business Sector. *G-Tech: Jurnal Teknologi Terapan*, *7*(4), 1498-1508. https://doi.org/10.33379/gtech.v7i4.3170

ISSN: 2716-3865 (Print), 2721-1290 (Online)

De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations*, 125-162. https://doi.org/10.1007/978-3-030-25918-1_5

Dharmada, T., Wiratama, J., & Faza, A. (2024). Leveraging COBIT 2019 Framework for Recommending ERP System Module Development at Cardboard Manufacturing Industry. *Journal of Information Systems and Informatics*, *6*(2), 1195-1214. https://doi.org/10.51519/journalisi.v6i2.764

Fianty, M. I., & Brian, M. (2023). Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company. *Journal of Information Systems and Informatics*, *5*(2), 568-579. https://doi.org/10.51519/journalisi.v5i2.492

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Ishlahuddin, A., Handayani, P. W., Hammi, K., & Azzahro, F. (2020, September). Analysing IT governance maturity level using COBIT 2019 framework: A case study of small size higher education institute (XYZ-edu). In *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)* (pp. 236-241). IEEE. https://doi.org/10.1109/IC2IE50715.2020.9274599

Jawad, M. M., Ali, M. H., Khaleel, A. A., & Hasan, M. F. (2023). Evaluating the performance of IT management under the implementation of the COBIT 2019 framework. *Eximia*, *12*, 18-36. https://doi.org/10.47577/eximia.v12i1.331

Johanning, V. (2023). *Organization and Management of IT: The New Role of IT and the CIO in Digital Transformation*. Springer Nature. https://doi.org/10.1007/978-3-658-39572-8

Lumingkewas, C., Mambu, J. Y., & Wahyudi, A. (2023). Identification of IT governance capability level of COBIT 2019 at the Kominfo City of Bitung, North Sulawesi. *TeIKa*, *13*(01), 1-15. https://doi.org/10.36342/teika.v13i01.3064

Pistikopoulos, E. N. (2024). Analysis of Information Technology Governance Management of Work Units in XYZ Agencies with the Cobit Framework 2019. *Join: Journal of Social Science*, *1*(1), 19-31. https://doi.org/10.59613/774nfg93

Rabii, A., Assoul, S., Ouazzani Touhami, K., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*, *28*(4), 627-644. https://doi.org/10.1108/ICS-03-2019-0039

Ramadhana, R., Izaac, B. V., Tangka, G. W., & Mambu, J. Y. (2023). Information Technology Governance Analysis Using the COBIT 2019 Framework at PT. Daya Adicipta Wisesa. *Jurnal Informasi dan Teknologi*, 141-146. https://doi.org/10.60083/jidt.v5i3.414

Solikhah, M. A., Magdalena, L., & Hatta, M. (2024). Implementation of the COBIT 2019 Framework on Information Technology Governance and Risk Management (Study Case: CV. Syntax Corporation Indonesia). *Eduvest-Journal of Universal Studies*, *4*(8). https://doi.org/10.59188/eduvest.v4i7.1504

Syahputra, M. H. A., & Sutomo, R. (2023). Analysis of IT Performance on Management HR of Equity Firm Using COBIT 5. *Journal Of Information Systems And Informatics*, *5*(2), 650-664. https://doi.org/10.51519/journalisi.v5i2.494

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards a review and comprehensive overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, 120743. https://doi.org/10.1016/j.techfore.2021.120743

Utomo, D., Wijaya, M., Suzanna, S., Efendi, E., & Sagala, N. T. M. (2022). Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A. *CommIT (Communication and Information Technology) Journal*, *16*(2), 129-141. https://doi.org/10.21512/commit.v16i2.8172

Widharto, P., Suhatman, Z., & Aji, R. F. (2022). Measurement of information technology governance capability level: a case study of PT Bank BBS. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *20*(2), 296-306. http://doi.org/10.12928/telkomnika.v20i2.21668

Yang, K. (2020). Unprecedented challenges, familiar paradoxes: COVID-19 and governance in a new normal state of risks. *Public Administration Review*, *80*(4), 657-664. https://doi.org/10.1111/puar.13248

ISSN: 2716-3865 (Print), 2721-1290 (Online)