INTENSIF, Vol.8 No.1 February 2024
ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks

Received:
27 September 2023
Accepted:
18 January 2024
Published:
1 February 2024

[1*]Yulia Darmi, [2]Sandhy Fernandez, [3]M Yoka Fathoni, [4]Sena Wijayanto
[1]Teknik Informatika, Universitas Muhammadiyah Bengkulu
[2,4]Sistem Informasi, Institut Teknologi Telkom Purwokerto
[3]Information Technology, Universiti Kuala Lumpur

E-mail: [1]yuliadarmi@umb.ac.id, [2]sandhy@ittelkom-pwt.ac.id, [3]fathoni.yoka@s.unikl.edu.my, [4]sena@ittelkom-pwt.ac.id
*Corresponding Author

Abstract—Information system security within XYZ University constitutes a vital component of its IT framework, exerting significant influence over security levels across all facets of the information systems. Among the numerous implemented information system services at the university, a considerable portion lacks active security measures within operational systems. In pursuit of achieving uniform governance, this study adopts the most recent COBIT 2019 framework. The primary objective of this research is to evaluate the degree to which current information system security management aligns with the process achievement values stipulated in the COBIT 2019 standard. This evaluation entails the calculation of maturity level values that gauge performance levels in managing information system security. Findings from the COBIT 2019 Design assessment conducted at XYZ University's LTIK reveal that individuals scoring above 80 or those requiring Capability Level 4 include APO12 and BAI10. Moreover, the calculation outcomes for each subdomain reveal the presence of 2 subdomains at Level 4, 4 subdomains at Level 3, 15 subdomains at Level 2, and 19 subdomains at Level 1. The identification outcomes underscore the existence of gaps within each domain. Particularly, the APO12 and BAI10 domains exhibit a gap spanning 2 levels.

Keywords— IT Governance; Information System Security; COBIT 2019

This is an open access article under the CC BY-SA License.

Corresponding Author:

Yulia Darmi,
Teknik Informatika,
Universitas Muhammadiyah Beng,
Email: yuliadarmi@umb.ac.id
ID Orchid: http://orcid.org/0009-0002-4709-8255

I. INTRODUCTION

Information technology has become a necessity for every company in today's age. With every advancement in information technology, the demand for security in its systems has increased to support the business needs of these companies [1], [2]. Information security is a crucial aspect of the operations of any university, as it helps protect the technological and information assets employed by the institution [3]. Information system security at XYZ University is an integral part of its IT, playing a crucial role in ensuring security across all information system sectors. However, despite implementing various information system services, many systems are lacking security measures, and the management of information system security lacks standardized practices, leading to overlaps in security management efforts. Another issue arises from the increasing number of information systems connected to the internet, which makes protecting these systems more complex and brings new challenges in designing appropriate governance in line with standards. Therefore, it is necessary to conduct an evaluation through performance measurement of information system security in the institution's information and communication technology department at XYZ University. Based on the conclusions drawn from the issues and objectives, there are research questions that will be analyzed to what extent XYZ University has successfully implemented the COBIT 2019 framework by measuring the current capability and also measuring the gap between the current state and the expected outcomes based on COBIT 2019 measurements.

IT governance is a process capable of designing a close determination regarding IT within a corporate environment to achieve the organization's desired objectives for the present time [4], [5], [6]. There are several standard models in information technology governance widely recognized for assessing the performance of IT governance. Some of them are The IT Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT), and ISO/IEC 27001 [7]. These three standards aim to ensure that the implementation of information technology within an organization aligns with expectations and mitigates risks. From these three standard models of IT governance, COBIT is chosen as the appropriate framework. COBIT provides the necessary components for building and managing information technology systems, such as processes, organizational structure, policies and procedures, information flow, culture and behavior, skills, and infrastructure [8], [9], [10]. COBIT assists organizations in considering crucial design factors when developing a suitable information technology governance system to address issues by grouping relevant components into governance and management. Furthermore, COBIT defines elements that describe the decisions to be made and how to execute them [11], [12], [13]. In 2018, the Information Systems Audit and

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

Control Association (ISACA) released the latest version of COBIT, namely COBIT 2019, with some new adjustments, including the use of design factors. These changes enable COBIT to be more easily adapted to specific contexts [14], [15], [16], [17].

COBIT represents an information technology framework created by the ISACA entity, aimed at aiding organizations in optimizing their IT assessments to strike a harmonious equilibrium between anticipated advantages, risk mitigation, and resource allocation [18], [19]. Comprising a series of documents outlining best practices for information technology governance, COBIT is crafted to assist users and management alike [20]. Its role lies in bridging the gap that exists among business risks, control requisites, and intricate technical IT-related aspects [21]. The core objective of this research is to gauge the extent of the current maturity level within system security, utilizing COBIT 2019 standards as a benchmark. This assessment is accomplished by computing the maturity level, which functions as a representation of the proficiency level in information system security [22], [23], [24], [25], [26].

II. RESEARCH METHOD

The chosen research methodology is analytical and descriptive in nature, with the primary objective of illustrating the current state of a particular phenomenon. This will be followed by a quantitative analysis approach. To carry out this study, the COBIT 2019 standard procedures will be employed as an analytical framework. The research will utilize a set of respondents, along with formulas to calculate maturity values and techniques for assessing scores. These tools will collectively facilitate the determination of maturity levels.

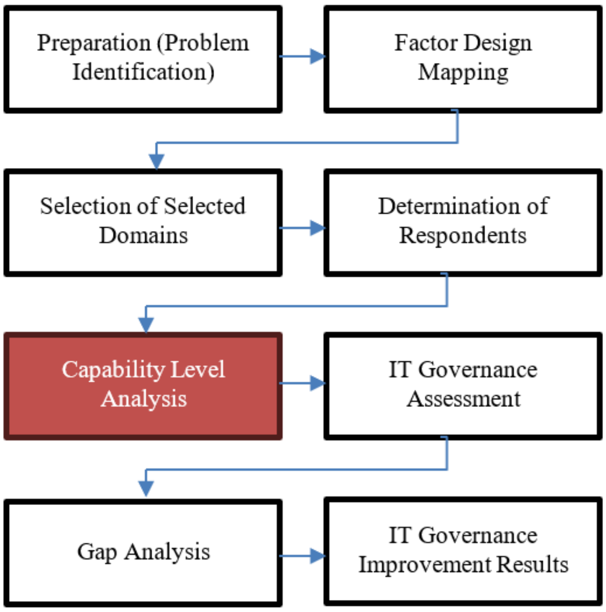
Preparation (Problem Identification)
Factor Design Mapping
Selection of Selected Domains
Determination of Respondents
Capability Level Analysis
IT Governance Assessment
Gap Analysis
IT Governance Improvement Results

Fig 1. Research Methodology

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

The data collection involves a literature review encompassing sources such as books, journals, articles, and the internet. Discussions are conducted to elucidate the theory and application of governance using the COBIT 2019 framework. Direct interviews are carried out with the leaders of the IT unit at XYZ University, focusing on the current state and management of information system security. The researcher also conducts observations by reviewing documents related to information system security. The administration of questionnaires aims to collect data by presenting a series of questions aligned with the COBIT 2019 standards that will be measured. Respondents in this study are selected based on relevant stakeholders, determined through mapping the RACI Chart to prioritize processes. The assessment of the rating for each subprocess is conducted using the NPLF method, based on all identified subprocess activities.

Based on the illustration of the research flow diagram, the process can be elucidated as follows: The initial phase involves executing the research plan, encompassing activities like problem identification. Subsequently, observations are conducted within XYZ University's Information and Communication Technology Institute, where the application's functioning is examined by monitoring the requisite documents related to the research. Following this, information regarding the specific case is accumulated to compare it against the model and procedure employed for in-depth design at various levels. The model's course of action to be adopted aligns with the design factors within the COBIT 2019 framework. This methodology is enacted through the analytical stages of the COBIT 2019 factor design. The subsequent segment involves the selection of pertinent components from the COBIT 2019 framework based on individual preferences. Within this segment lies the comprehensive process sequence of all COBIT 2019 processes [27], [28], [29], [30], [31].

Determination on the activity starts the domain that has been selected will create questions in the questionnaire given to correspondents. The processes from the selected domains are taken from activities in the COBIT 2019 framework. Each scope may differ depending on the activities they carry out together with the COBIT 2019 framework. After the next selected area is identified, it is determined which respondent is the subject of this study. When inquiries are directed towards the predetermined activities within a specific field, aiming to conduct tests on the designated list of participants, the primary objective of this process is to obtain the outcomes of these activities. Concluding the research plan's progression, the ultimate phase involves selecting the goals for capability levels. These chosen objectives will subsequently serve as benchmarks for the level identification process. The outcomes pertaining to competency levels are derived from the domain mapping findings. The necessary level of accomplishment to be reached will be ascertained based on these outcomes [32], [33], [34], [35], [36].

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

Perform an examination of the acquired documents and oversee the objectives that will ultimately be presented to the Information and Communication Technology Institute at XYZ University. This oversight is pivotal for the finalization of the process aimed at identifying the level of management for information system security. The document analysis procedure encompasses both the computation of capability levels and the execution of gap analysis. Capability level calculations serve the purpose of evaluating the status of information system security in relation to its management. Meanwhile, gap analysis entails a comparative assessment between the attained accomplishments and the anticipated achievements within the context of XYZ University's Information and Communication Technology unit.

III. RESULT AND DISCUSSION

By combining all the design factor values in COBIT 2019 which have been carried out in the factor design mapping stage, all the resulting domains are then combined into a governance design as illustrated in Figure 2.

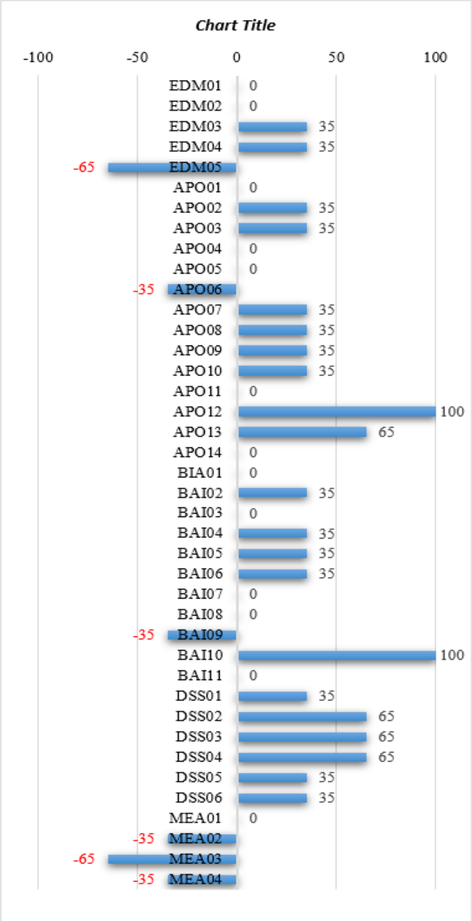

Fig 2. Results of All Design Factors

Figure 2 depicts the outcomes of the COBIT 2019 implementation at XYZ University's LTIK. This governance design yields a process with suggested proficiency levels. COBIT 2019 specifies that achieving a proficiency level of 80 or higher requires a certain degree of expertise. When the proficiency score reaches 50 or higher, a proficiency level of 3 is anticipated. Scores exceeding 25 mandate a competency level of 2, whereas a full score below 25 corresponds to the need for the process to reach competency level 1. The subsequent findings pertain to the administration of LTIK XYZ University. Based on the outcomes derived from the 2019 COBIT Design assessment at LTIK XYZ University, it is discernible that individuals who achieve scores surpassing 80 or are required to attain Capability Level 4 include APO12 and BAI10.

After obtaining two important domains from the results of the COBIT 2019 design factors, the next step is to select respondents to fill out questions in each of these domains. There were three respondents from XYZ University who were involved, namely the Head of LTIK, the Head of the Hardware Section and the Head of the Software Section. In calculating the level of ability will be calculated from the two domains that get a score of more than 85. Assessment is based on the provisions if the level of ability achieved is less than 15% then the result is N (Not Achieved). If the ability level reaches between 15% and 50%, then the result is P (Partially Achieved). If it reaches between 50% and 85% then the result is L (Major Achieved). And if it reaches more than 85% then the result is F (Fully Achieved). If the result is F, then you can proceed to the next level of ability. However, if the result does not reach F, the ability level will only stop at that level. The results of the overall factor design statement, selected two priority management objectives with a score of more than 80, namely APO12 and BAI10, both of which have a suggested ability level of 4. After selecting from the two domains, further calculations will be carried out, namely determining the attainment of the ability level of the two domains the. The results of measuring the ability level can be seen in the following table.

Table 1. Level Capability Assessment 1 APO12

Responden	Activity Value	Number of Activities	Capability
R1	1	1	100%
R2	1	1	100%
R3	1	1	100%
		Total	100% (F)

Table 1 shows the results of APO12 activities at Capability Level 1. In the process of calculating the value at Capability Level 1 reaching 100% or F (Fully Achieved), an assessment is made for the next level, namely Level 2. APO12 activities at Capability Level 2 can be seen in Table 2 .

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

Table 2. Level Capability Assessment 2 APO12

Responden	Activity Value	Number of Activities	Capability
R1	6	6	100%
R2	5	6	83%
R3	5	6	83%
		Total	88% (F)

Table 2 shows the results of APO12 activities at Capability Level 2. In the process of calculating the value at Capability Level 2 reaching 88% or F (Fully Achieved), an assessment is made for the next level, namely Level 3. The results of APO12 activities at Capability Level 3 can be seen in Table 3.

Table 3. Level Capability Assessment 3 APO12

Responden	Activity Value	Number of Activities	Capability
R1	16	18	88%
R2	13	18	72%
R3	12	18	66%
		Total	75% (L)

Table 3 shows the results of APO12 activities at Capability Level 3. In the process of calculating scores at Capability Level 3, the results only reach 75% or L (Mostly Achieved). Therefore, it is not possible to evaluate at the next level, namely Level 4. Based on the table it can be concluded that the APO12 domain obtains a capability value at Level 2.

Table 4. Level Capability Assessment 1 BAI10

Responden	Activity Value	Number of Activities	Capability
R1	1	1	100%
R2	1	1	100%
R3	1	1	100%
		Total	100% (F)

Table 4 shows the results of BAI10 activities at Capability Level 1. In the process of calculating scores at Capability Level 1 reaching 100% or F (Fully Achieved), an assessment is made for the next level, namely Level 2. BAI10 activities at Ability Level 2 can be seen in Table 5.

ISSN: 2580-409X (Print) / 2549-6824 (Online)
DOI: https://doi.org/10.29407/intensif.v8i1.21221

Table 5. Level Capability Assessment 2 BAI10

Responden	Activity Value	Number of Activities	Capability
R1	5	5	100%
R2	4	5	80%
R3	4	5	80%
		Total	86% (F)

Table 5 shows the results of BAI10 activities at Capability Level 2. In the process of calculating scores at Capability Level 2 it reaches 86% more or F (Fully Achieved), then an assessment is carried out for the next level, namely Level 3. The results of BAI10 activities at Capability Level 3 can be seen in Table 6.

Table 6. Level Capability Assessment 3 BAI10

Responden	Activity Value	Number of Activities	Capability
R1	5	6	83%
R2	5	6	83%
R3	3	6	50%
		Total	72% (L)

Table 6 shows the results of BAI10 activities at Ability Level 3. In the process of calculating scores at Ability Level 3, the results only reach 72% or L (Most Achieved). Therefore, it is not possible to evaluate at the next level, namely Level 4. Based on the table, it can be concluded that the BAI10 domain obtains a capability value at Level 2. Based on the results of the ability levels in the 2 domains, namely APO12 and BAI10, it was obtained that the ability levels were achieved by XYZ University. Furthermore, we can analyze the gap (gap) between the expected target level and the level of ability that has been achieved at this time. The results of the gap analysis are listed in Table 7.

Table 7. Domain Gap Results

Domain	Target Capability Level	Current Capability Level	Gap
APO12	4	2	2
BAI10	4	2	2

The results of the gap analysis are shown in table 7, where there is a difference of 2 levels in the APO12 domain and a difference of 2 levels in the BAI10 domain. To fill the gap at that level of ability, every element that must be met from each predetermined level must be met.

This research has potential constraints that may arise, both in the analysis process and upon completion. One such challenge is maintaining the sustainability of COBIT 2019 implementation, particularly when there are changes in leadership, shifts in organizational priorities, or alterations in the business environment. Changes in the external environment, for instance, can impact the relevance and effectiveness of implementing COBIT 2019.

IV. CONCLUSION

The results of the identification of the management design level at XYZ University show that the calculation of the capability level in the APO12 domain and the BAI10 domain is at Level 2. This indicates that the processes in these domains have been implemented and have succeeded in achieving organizational goals. aim properly. However, from the identification results, it appears that there are gaps in each domain. The APO12 and BAI10 domain gap has 2 levels. To improve the quality of service management, it is advisable to carry out activities that are already at each current level of ability in order to achieve the expected level of ability. For example, in the APO12 domain, the expected target ability level is 4, but currently it has only reached level 2. In the BAI10 domain, the expected target ability level is also 4, but currently it has only reached level 2. With the implementation of existing activities, it is expected the level of ability in each domain can be increased according to predetermined targets.

The activities that can be carried out to reach the next level are creating and consistently updating Information and Technology (I&T) risk scenarios, exposure to I&T-related losses, and reputation risk scenarios, which include combined scenarios involving cascading and coincidental threat types and events. Determine specific control activities and capabilities for detection expectations. Explain and reach a consensus on the scope and complexity of configuration management, defining configurable services, assets, and infrastructure items to combine.

Author Contributions: *Yulia Darmi*: Conceptualization, Methodology, Writing - Original Draft, Writing - Review & Editing, Supervision. *Sandhy Fernandez*: Software, Investigation, Data Curation, Writing - Original Draft. *M Yoka Fathoni*: Review, Data Curation. *Sena Wijayanto*: Investigation, Review.

All authors have read and agreed to the published version of the manuscript.

Funding: This research received no specific grant from any funding agency.

Conflicts of Interest: The authors declare no conflict of interest.

Data Availability: The data cannot be openly shared for the protection of study participant privacy.

Informed Consent: There were no human subjects.

Animal Subjects: There were no animal subjects.

ORCID:
Yulia Darmi: http://orcid.org/0009-0002-4709-8255
Sandhy Fernandez: http://orcid.org/0009-0001-7403-6853
M Yoka Fathoni: http://orcid.org/0000-0001-7651-6351
Sena Wijayanto: http://orcid.org/0000-0003-4406-4447

REFERENCES

[1] M. R. Asghar, Q. Hu, and S. Zeadally, “Cybersecurity in industrial control systems: Issues, technologies, and challenges,” Computer Networks, vol. 165, Dec. 2019, doi: 10.1016/j.comnet.2019.106946.

[2] I. Lee, “Cybersecurity: Risk management framework and investment cost analysis,” Bus Horiz, vol. 64, no. 5, pp. 659–671, Sep. 2021, doi: 10.1016/j.bushor.2021.02.022.

[3] I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, “Web vulnerability assessment and maturity model analysis on Indonesia higher education,” in Procedia Computer Science, Elsevier B.V., 2019, pp. 1165–1172. doi: 10.1016/j.procs.2019.11.229.

[4] R. M. Tawafak, A. Romli, S. I. Malik, and M. Shakir, “IT Governance Impact on Academic Performance Development,” International Journal of Emerging Technologies in Learning, vol. 15, no. 18, pp. 73–85, 2020, doi: 10.3991/ijet.v15i18.15367.

[5] S. Fernandez, M. Imanullah, M. Y. Fathoni, and P. Pahrizal, “Utilization of the COBIT 2019 framework to identify the level of governance in internet services,” JURNAL INFOTEL, vol. 14, no. 3, pp. 188–195, Aug. 2022, doi: 10.20895/infotel.v14i3.791.

[6] A. Irsheid, A. Murad, M. Alnajdawi, and A. Qusef, “Information security risk management models for cloud hosted systems: A comparative study,” in Procedia Computer Science, Elsevier B.V., 2022, pp. 205–217. doi: 10.1016/j.procs.2022.08.025.

[7] G. Breda and M. Kiss, “Overview of information security standards in the field of special protected industry 4.0 areas & industrial security,” in Procedia Manufacturing, Elsevier B.V., 2020, pp. 580–590. doi: 10.1016/j.promfg.2020.03.084.

[8] D. Sulistyowati, F. Handayani, and Y. Suryanto, “Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS,” International Journal On Informatics Visualization, vol. 4, no. 2, 2020.

[9] L. Ramadani, B. Maulidya Izzati, and Y. Mayagita Tarigan, “Managing Information Technology Risks to Achieve Business Goals: A Case of Pharmaceutical Company,” International Journal On Informatics Visualization, vol. 7, no. 2, pp. 345–355, 2023, [Online]. Available: www.joiv.org/index.php/joiv

[10] M. Ikhsan, A. P. Widodo, and K. Adi, “Systematic Literature Review on Corporate Information Technology Governance in Indonesia using Cobit 2019,” Prisma Sains : Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram, vol. 9, no. 2, p. 354, Dec. 2021, doi: 10.33394/j-ps.v9i2.4370.

[11] E. Amore, T. Dilger, C. Ploder, R. Bernsteiner, and M. Mezzenzana, “Leverage the COBIT 2019 Design Toolkit in an SME Context: A Multiple Case Study,” KnE Social Sciences, Feb. 2023, doi: 10.18502/kss.v8i1.12636.

[12] L. Jaime and J. Barata, “How can FLOSS Support COBIT 2019? Coverage Analysis and a Conceptual Framework,” Procedia Comput Sci, vol. 219, pp. 680–687, 2023, doi: 10.1016/j.procs.2023.01.339.

[13] R. Hanafi, M. Munir, S. Suwatno, and C. Furqon, “Identification of IT Governance and Management Objectives and Target Process Capability Level in Government Institution,”

INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, vol. 7, no. 2, pp. 290–308, Aug. 2023, doi: 10.29407/intensif.v7i2.20108.

[14] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, “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 2020, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 236–241. doi: 10.1109/IC2IE50715.2020.9274599.

[15] A. Gerl, M. Von Der Heyde, R. Groß, R. Seck, and L. Watkowski, “Applying COBIT 2019 to IT Governance in Higher Education,” INFORMATIK, 2020.

[16] G. Bagus, R. Francolla, G. Rihart Mandoya, M. D. Walangitan, and E. Lompoliu, “Information Technology Governance Audit Using The COBIT 2019 Framework at XYZ Institution,” DESEMBER 2022 Cogito Smart Journal |, vol. 8, no. 2, 2022.

[17] M. Yasin, A. Akhmad Arman, I. J. M. Edward, and W. Shalannanda, “Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ),” in Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/TSSA51342.2020.9310875.

[18] S. Slapničar, T. Vuko, M. Čular, and M. Drašček, “Effectiveness of cybersecurity audit,” International Journal of Accounting Information Systems, vol. 44, Mar. 2022, doi: 10.1016/j.accinf.2021.100548.

[19] S. Lee, F. J. Costello, and K. C. Lee, “Hierarchical balanced scorecard-based organizational goals and the efficiency of controls processes,” J Bus Res, vol. 132, pp. 270–288, Aug. 2021, doi: 10.1016/j.jbusres.2021.04.038.

[20] M. Malatji, A. Marnewick, and S. von Solms, “Validation of a socio-technical management process for optimising cybersecurity practices,” Comput Secur, vol. 95, Aug. 2020, doi: 10.1016/j.cose.2020.101846.

[21] A. Mukhopadhyay and S. Jain, “A framework for cyber-risk insurance against ransomware: A mixed-method approach,” Int J Inf Manage, vol. 74, Feb. 2024, doi: 10.1016/j.ijinfomgt.2023.102724.

[22] A. Irhandayaningsih, “Performance Measurement of Information Technology Governance in the Library of Diponegoro University Using COBIT Assessment Framework,” in E3S Web of Conferences, EDP Sciences, Nov. 2020. doi: 10.1051/e3sconf/202020215001.

[23] H. Yubo, “IT Risk Control for Internet Finance Based on COBIT,” in Proceedings - 2020 International Conference on Big Data and Artificial Intelligence and Software Engineering, ICBASE 2020, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 275–278. doi: 10.1109/ICBASE51474.2020.00064.

[24] Rini Audia and B. Sugiantoro, “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), vol. 11, no. 1, pp. 152–161, Aug. 2022, doi: 10.14421/ijid.2022.3381.

[25] F. Ajismanto and S. Surahmat, “Information Technology Governance Analysis Of Stmik Palcomtech In The New Normal Era Using Cobit 2019 Method,” Journal of Computer Networks, Architecture and High Performance Computing, vol. 3, no. 2, pp. 263–272, Nov. 2021, doi: 10.47709/cnahpc.v3i2.1097.

[26] G. Toaza, C. Montenegro, and C. Salazar, “Designing an I&T Governance System in the Context of Strategic Public Sector Based on COBIT 2019 Framework. Case Study in a Developing Country,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Aug. 2022, pp. 401–406. doi: 10.1145/3564858.3564920.

[27] D. Henriques, R. Almeida, R. Pereira, M. M. da Silva, and I. S. Bianchi, “How IT governance can assist iot project implementation,” International Journal of Information

Systems and Project Management, vol. 8, no. 3, pp. 25–45, 2020, doi: 10.12821/ijispm080302.

[28] R. Adhitya Nugraha and R. Syaidah, “Smart Campus Governance Design for XYZ Polytechnic Based on COBIT 2019,” International Journal On Informatics Visualization, 2022, [Online]. Available: www.joiv.org/index.php/joiv

[29] A. Safitri, I. Syafii, and K. Adi, “Measuring the Performance of Information System Governance using Framework COBIT 2019,” Int J Comput Appl, vol. 174, no. 31, pp. 23–30, Apr. 2021, doi: 10.5120/ijca2021921253.

[30] D. Utomo, M. Wijaya, and N. Tri Maretta Sagala, “Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A,” 2022.

[31] M. Lestari, A. Iriani, and H. Hendry, “Information Technology Governance Design in DevOps-Based E-Marketplace Companies Using COBIT 2019 Framework,” INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi, vol. 6, no. 2, pp. 233–252, Aug. 2022, doi: 10.29407/intensif.v6i2.18104.

[32] M. M. Alratrout, B. A. Thani, N. Taleb, and R. Said, “The Challenges of Compliance it Governance Frameworks in the UAE,” International Journal of Emerging Multidisciplinaries, 2022, doi: 10.54938/ijemdcsai.2022.01.2.140.

[33] H. Nurcahya, E. Setiawan, and B. Permana, “Information Technology Governance Audit Using COBIT Framework 2019 (Case Study: Mandiri University),” Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 2022, doi: 10.33258/birci.v5i1.4566.

[34] J. Grabis et al., “The Information System Security Governance Tasks in Small and Medium Enterprises,” 2020.

[35] S. Samsinar and R. Sinaga, “Information Technology Governance Audit at XYZ College Using COBIT Framework 2019,” Berkala Sainstek, vol. 10, no. 2, p. 58, Jun. 2022, doi: 10.19184/bst.v10i2.30325.

[36] V. Kasma Septiyana, S. Sutikno, and K. Surendro, “Design of e-Government Security Governance System Using COBIT 2019,” in International Conference on ICT for Smart Society (ICISS), International Conference on ICT for Smart Society (ICISS), 2019.