Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 111–120
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.45011
©2025. The Author(s). This is an open acces article under cc-by-sa

Analysis of Information Technology Governance Priorities at PTKIN Using The COBIT 2019 Framework

Nur Aeni Hidayah[1*], Junaidi[2], Elvi Fetrina[3], Suci Ratnawati[4]

***Abstract*—Risk management is a part of information technology (IT) governance, enabling organizations to safeguard their information assets effectively and efficiently. It involves identifying potential risks, planning mitigation strategies, and establishing relevant policies. An interview with the Head of Pustipanda at Syarif Hidayatullah State Islamic University (SIU) Jakarta revealed that the university underwent an IT governance audit by the National Cyber and Crypto Agency in 2020, with results indicating the need for significant improvements. Given the critical role of the Academic Information System (AIS) as a strategic IT asset in higher education, effective management is essential. This study aims to evaluate the IT governance maturity of Pustipanda using the COBIT 2019 framework and to identify key governance domains that should be prioritized for improvement. The study focuses on the IT governance of Pustipanda Syarif Hidayatullah SIU Jakarta, selected as a sample from the broader population of PTKIN (State Islamic Religious Colleges) in Indonesia. Using the COBIT 2019 framework, the research identifies 22 IT governance domains prioritized for implementation, with six domains categorized as top priority. These findings provide actionable insights for IT governance enhancement, particularly in academic institutions. The methodology presented can serve as a reference for other PTKIN to assess and prioritize IT governance domains according to their specific organizational needs, supporting the development of more secure, efficient, and well-governed IT environments in higher education institutions.**

***Index Terms*—Risk management, IT governance, COBIT 2019, UIN syarif hidayatullah jakarta.**

Received: 19 February 2025; Revised: 9 March 2025; Accepted: 10 May 2025
*Corresponding author

[1*]Nur Aeni Hidayah, UIN Syarif Hidayatullah Jakarta, Indonesia (e-mail: nur.aeni@uinjkt.ac.id).
[2]Junaidi, UIN Syarif Hidayatullah Jakarta, Indonesia (e-mail: junaidi_fst@uinjkt.ac.id).
[3]Elvi Fetrina, UIN Syarif Hidayatullah Jakarta, Indonesia (e-mail: elvifetrina@uinjkt.ac.id).
[4]Suci Ratnawati, UIN Syarif Hidayatullah Jakarta, Indonesia (e-mail: suci.ratnawati@uinjkt.ac.id).

I. Introduction

The development of information technology today has made it not only a tool for supporting business processes but also a strategic instrument that aids organizational business strategies and enhances service quality [1]. As the role of information technology in organizations continues to grow, information is now considered a highly valuable asset. In the organizational context, information is one of the intangible assets that must be protected to ensure the organization's sustainability [2]. In the use of information systems designed to collect, process, and present information, the potential for unwanted incidents is quite significant. Therefore, risk management in the use of information systems is crucial to protect information assets from threats that may harm the organization [3]. Consequently, risk management, which includes managing every asset related to information, becomes an essential part of information technology governance.

Risk management, which is a part of information technology governance, is necessary for organizations as it determines the security of information assets in the most effective and cost-efficient manner [4]. Risk management involves risk assessment, also known as risk analysis, to evaluate how frequently risks occur and their potential impact. This risk assessment includes identifying and evaluating risks related to the confidentiality, integrity, and availability of information systems and resources [5]. Risk assessment is a component of information system risk management conducted to assess the likelihood of threats and vulnerabilities to information systems and their assets. The presence of risk management in the management of an organization's information assets is crucial. Understanding risks and planning actions to mitigate those risks, as well as formulating policies to address them, are fundamental aspects of risk management.

Awareness of the importance of information system security and its associated assets within an organization, along with the potential impacts of system failures, still seems to be lacking in many organizations. Evaluating how an organization implements risk management is essential to determine the organization's capability in managing risks, especially for

critical information technology assets.

The Academic Information System (AIS) is an information system used across all educational levels, from primary and secondary education to higher education. The objective of developing information systems is to achieve successful application in the institutions that use them, as well as by their developers [6]. According to [7], AIS serves as a medium to assist in decision-making, providing a competitive advantage and supporting higher education activities. Several researchers, such as [8] and [9], have conducted extensive studies on academic information systems. They argue that the use of information systems helps universities improve service quality and educational standards proportionally and in line with academic expectations. In higher education, service quality is a crucial aspect that contributes to a university's competitive advantage.

Given the critical role of AIS, it must be well-managed by higher education institutions. All academic activities are recorded within the system, making effective risk management for SIA a necessity. Any incident affecting the SIA can significantly impact university operations. This has become even more evident during the COVID-19 pandemic, which has restricted human movement due to social and physical distancing measures. Information technology has played a vital role as a solution to these restrictions across various sectors, including education, governance, economy, and healthcare. As higher education institutions, PTKIN (State Islamic Higher Education Institutions) have adapted to government policies, as outlined in the Ministry of Education and Culture Circular No. 36962/MPK.A/HK/2020, by implementing remote learning through the Academic Information System. Consequently, AIS has become the backbone of academic activities at PTKIN.

While the importance of information technology and its strategic role in organizations, particularly in higher education, is widely acknowledged, a critical gap exists in the effective management of risks associated with Academic Information Systems (AIS) within State Islamic Higher Education Institutions (PTKIN). As demonstrated during the COVID-19 pandemic, AIS has become the backbone of academic operations, handling sensitive student data, academic records, and crucial administrative processes. However, many PTKINs may lack a comprehensive understanding of the specific vulnerabilities and threats to their AIS, leading to potential security breaches, data loss, and operational disruptions. This deficiency is compounded by the unique characteristics of PTKINs, which often integrate Islamic values and principles into their academic and administrative practices, potentially introducing distinct risk factors that require tailored risk management strategies. Despite the recognized criticality of SIA, there is a lack of empirical research that systematically evaluates and addresses the specific risk management practices and challenges within PTKINs. This research gap highlights the need for a focused investigation to identify, assess, and propose effective risk mitigation strategies tailored to the unique context of SIA within these institutions.

II. Related Work

Numerous studies have been conducted on Academic Information Systems, including research on the design and implementation of SIA, its effectiveness, and user acceptance. For example, [10] conducted a study titled "Evaluation of the Implementation of Academic and Financial Information Systems on Student Satisfaction." The study aimed to assess the implementation of academic and financial information systems at IBIK and evaluate student satisfaction with their application. The findings revealed numerous issues in system implementation, which in turn affected student satisfaction with the academic and financial information systems.

Research on risk management using the Octave Allegro method has also gained significant attention. Studies by [11] and [12] applied this method to assess information asset risks in universities, demonstrating that high-risk factors can disrupt the sustainability of information technology utilization. Other research, such as that by [13] and [14], mapped risk areas in academic information systems and provided risk mitigation recommendations. Additionally, some studies have linked IT risks to information vulnerabilities, as seen in the works of [15] and [16], which identified key areas requiring management to maintain information security.

Further studies related to COBIT 2019 have been conducted, such as [17], which analyzed and designed IT governance using the COBIT 2019 framework at PT XYZ. This research identified five critical processes for evaluating PT XYZ: DSS02, DSS03, DSS05, BAI09, and MEA03. Additionally, [18] conducted a study aimed at designing an IT governance system for a hotel, identifying key processes such as BAI05, BAI06, BAI07, BAI11, BAI02, BAI07, BAI02, and BAI03, each with capability targets at levels 3 and 4.

There is also studies explored the IT governance model for e-Marketplace companies [19], a sector characterized by 24/7 operations and a strong consumer-centric focus. Employing a mixed-method approach and the COBIT 2019 framework, the research identified six critical IT processes—APO03, APO04, BAI04, BAI06, BAI11, and DSS03—as essential for effective governance, all achieving a capability level of 4. These processes, aligned with DevOps principles, are crucial for managing enterprise architecture, innovation, availability, IT changes, projects, and problem resolution within the e-Marketplace environment.

There's research investigated the role of IT governance in streamlining business operations within a printing machine distribution company [20], focusing on addressing issues related to inventory data accuracy and knowledge management. Using the COBIT 2019 framework and qualitative data collected through interviews, the study identified gaps in the capability levels of APO11, BAI08, and DSS06. The findings emphasized the necessity for enhancing IT knowledge management and procedural training to elevate these processes to the desired capability levels, thereby improving overall organizational quality and efficiency.

Based on the discussion above, the researcher is interested in assessing the priority of IT governance, particularly risk

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 111–120
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.45011
©2025. The Author(s). This is an open acces article under cc-by-sa

management and risk analysis of AIS at PTKIN. Data obtained from interviews with the Head of Pustipanda at UIN Syarif Hidayatullah Jakarta revealed that UIN Syarif Hidayatullah was previously audited for IT governance by the National Cyber and Encryption Agency in 2020. The audit results indicated that IT governance was still unsatisfactory, highlighting the need for improvements. Since UIN Syarif Hidayatullah was the only PTKIN included in the audit sample, the researcher has chosen it as the research object. The expectation is that the research findings will serve as a benchmark or best practice for implementing risk management in academic information system services within PTKIN institutions across Indonesia.

III. Research Method

This research is an empirical study conducted by the researcher using the COBIT 2019 Framework. The selection of this framework is based on the consideration that the researcher aims to identify the system design factors in an institution by utilizing the 11 design factors of COBIT 2019 as a quantitative approach. This study is conducted from September to November 2021. The selected PTKIN (State Islamic Religious Higher Education Institution) in Indonesia is Syarif Hidayatullah State Islamic University Jakarta, with the relevant unit being Pustipanda.

In this study, the researcher uses the population of PTKIN in Indonesia. The chosen sample is Pustipanda Syarif Hidayatullah SIU Jakarta because, in 2020, Pustipanda Syarif Hidayatullah SIU was one of the institutions selected to participate in the Incident Handling Maturity Level (TMPI) assessment by the National Cyber and Crypto Agency (BSSN). Additionally, this sample consists of units and human resources responsible for the Academic Information System of Syarif Hidayatullah SIU Jakarta, commonly known as AIS SIU Jakarta.

Figure 1 shows the research stages from formulating the problem to design modelling. The data collection techniques used in this research include interviews, FGD, literature studies, and observation. Interviews are conducted through focus group discussions (FGD) with the Head of the IT Unit and staff regarding IT risk management. These interviews aim to gather real-world data on risk management practices. In conducting interviews with both the Head of the IT Unit, staff, and experts, the researcher utilizes recording tools, either through online meeting platforms or a set of structured questions answered during the interview session. If a recording device is used, the researcher will perform verbatim transcription of the interview results.

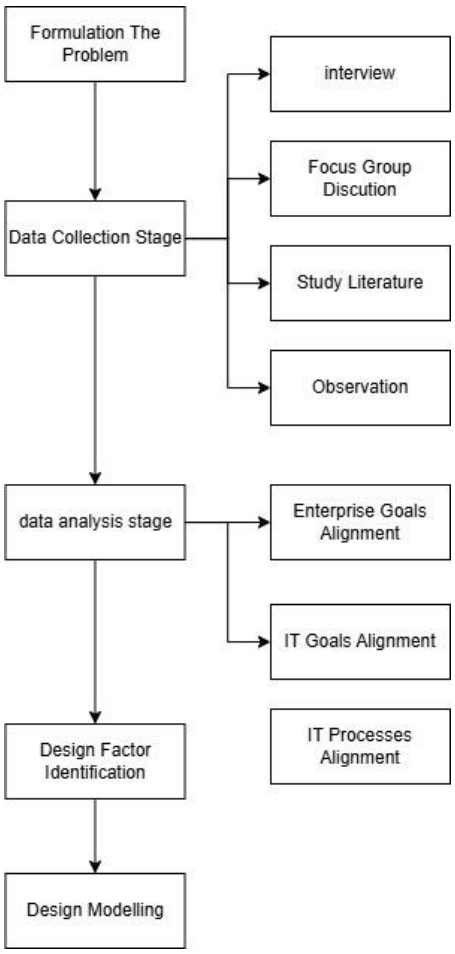

Fig. 1. Research stages.

The literature study in this research involves exploring theories, knowledge, and information related to the research topic, sourced from books, online articles, and research journals, both domestic and international. Lastly, the survey is conducted to identify the system design factors in Pustipanda UIN Syarif Hidayatullah Jakarta and provide risk management recommendations. This allows for an assessment of the current conditions in the implementation of risk management in the Academic Information System (AIS) services of SIU Jakarta. The instrument used for the survey is a questionnaire designed based on the COBIT 2019 framework.

This research applies an analysis using the COBIT 2019 Framework, in which the researcher evaluates the factors influencing the governance system design at UIN Syarif Hidayatullah Jakarta. This assessment aims to determine the institution's success level in utilizing IT. The evaluation is conducted using a questionnaire based on the COBIT 2019 framework. The results of this analysis will serve as the foundation for further research approaches.

IV. RESULT

The assessment of IT governance priorities is necessary to determine the governance areas that have been prioritized by Pustipanda. This evaluation will identify the governance domains that are the primary focus of Pustipanda, especially those related to risk management in the implementation of the Academic Information System (SIA).

A. Enterprise Strategy

The assessment of design factors in Fig. 2 serves as input for determining priority governance areas or domains related to enterprise strategy. The strategy archetypes consist of Growth/Acquisition, Innovation/Differentiation, Cost Leadership, and Client Services/Stability. The assessment of these design factors serves as input for prioritizing IT governance areas or domains aligned with enterprise strategy.

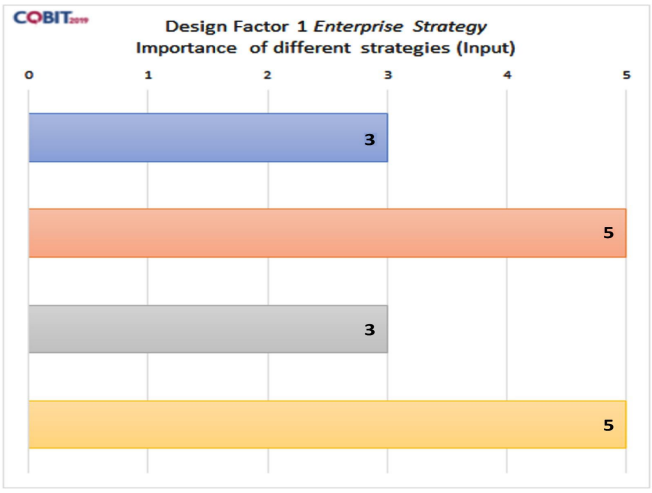

Fig. 2. Assessment of design factor enterprise strategy by respondents.

Figure 3 presents the output of the first design factor assessment, highlighting several key governance domains/areas, including APO 04, APO 08, APO 09, APO 11, APO 12, BAI 04, BAI 08, DSS 02, DSS 03, and DSS 04.

B. Enterprise Goals

In Fig. 4, it can be seen that the enterprise goals design factor consists of 13 assessed factors, of which 9 factors have received the highest level of importance (a score of 5) these are compliance with external law and regulator, quality of financial information, customer oriented services orientation, business continuity and availability, quality of information management, staff skills, motivation and productivity, compliance with internal policies, manage digital transformation programs dan product and business innovation.

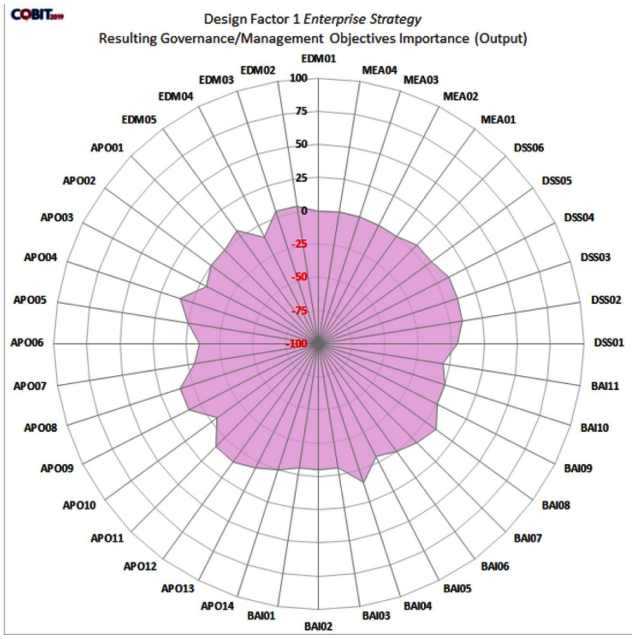

Fig. 3. IT governance areas/domains related to DF 01.

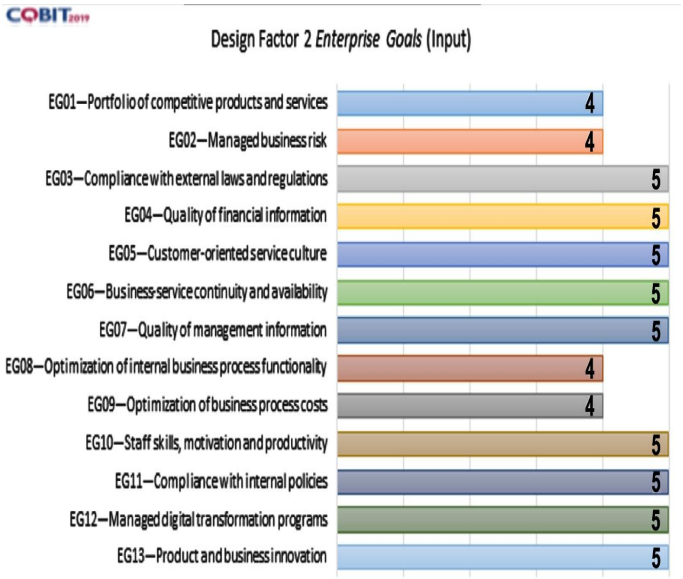

Fig. 4. Design factor enterprise goals assessment.

This score determines the IT governance priority areas at Pustipanda. The priority areas/domains are APO 04, APO 08, APO 09, APO 12, BAI 04, BAI 08, DSS 02, DSS 03, and DSS 04. These priority areas are illustrated in Figure 5. These areas are the main focus in building IT governance at UIN Syarif Hidayatullah.

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 111–120
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.45011
©2025. The Author(s). This is an open acces article under cc-by-sa

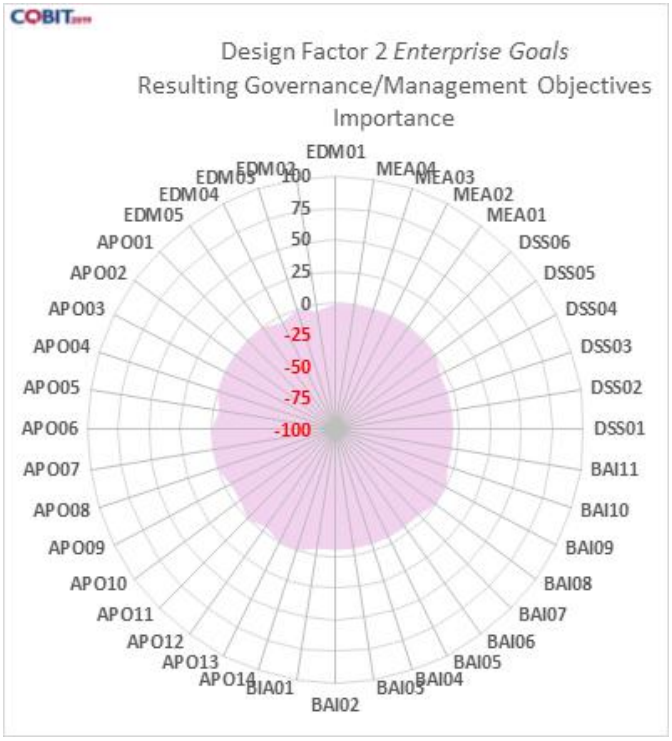

Fig. 5. IT governance areas/domains related to DF 02.

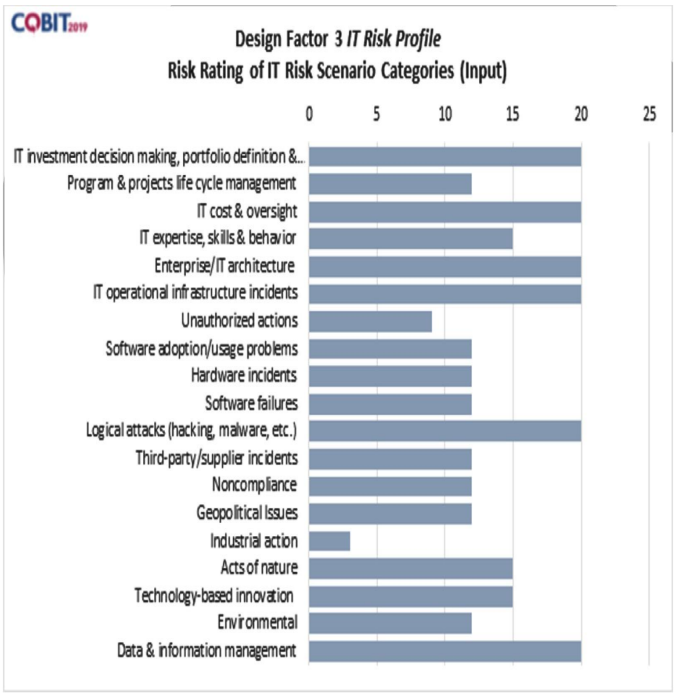

Fig. 6. IT risk profile design factor assessment.

C. IT Risk Profile

In the figure 7, we can see the results indicate that IT governance priorities lie within the domains or areas of EDM 01, EDM 02, EDM 03, EDM 04, EDM 05, APO 01, APO 02, APO 03, APO 04, APO 05, APO 06, APO 08, BAI 02, BAI 06, DSS 02, DSS 06, MEA 01, and MEA 02. These priority assessments can serve as guidelines for developing IT governance at SIU Syarif Hidayatullah, particularly in IT risk management. Considering the prioritized domains related to Pustipanda's IT Risk Profile design factor (Fig. 6), it is evident that numerous domains need to be implemented. Therefore, a phased approach to designing and developing IT governance is necessary to ensure the proper implementation of all processes within these domains.

C. IT Relate Issues

This design factor is associated with issues in IT use and governance. There are 20 critical issues that need to be assessed as input for determining priority governance domains (Fig. 8).

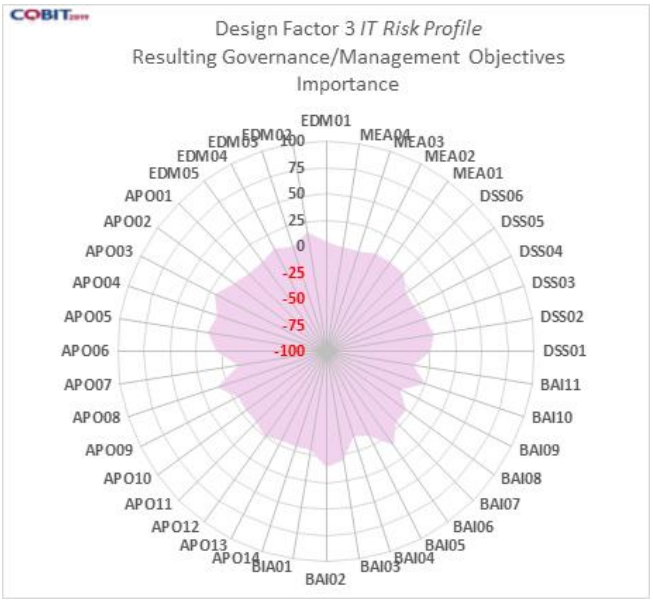

Fig. 7. IT governance areas/domains related to DF 03.

In the Fig. 9, there are 11 issues have been identified as major concerns for Pustipanda as the IT management unit at UIN Syarif Hidayatullah, as indicated by their highest importance ratings. The data processing results show that the priority IT governance domains at Pustipanda include BAI 01, BAI 10, and DSS 04.

E. Threat Landscape

A threat is an action or event that can harm a company or organization, resulting in financial loss, effort expenditure, missed business opportunities, reputational damage, and, in the worst case, bankruptcy. Threats can enter through various vulnerabilities. In the threat landscape design factor in the Fig. 10, Pustipanda evaluates that 60% of threats have a high impact, while 40% have a low impact (Fig. 9). This indicates that Pustipanda places significant attention on high-impact threats.

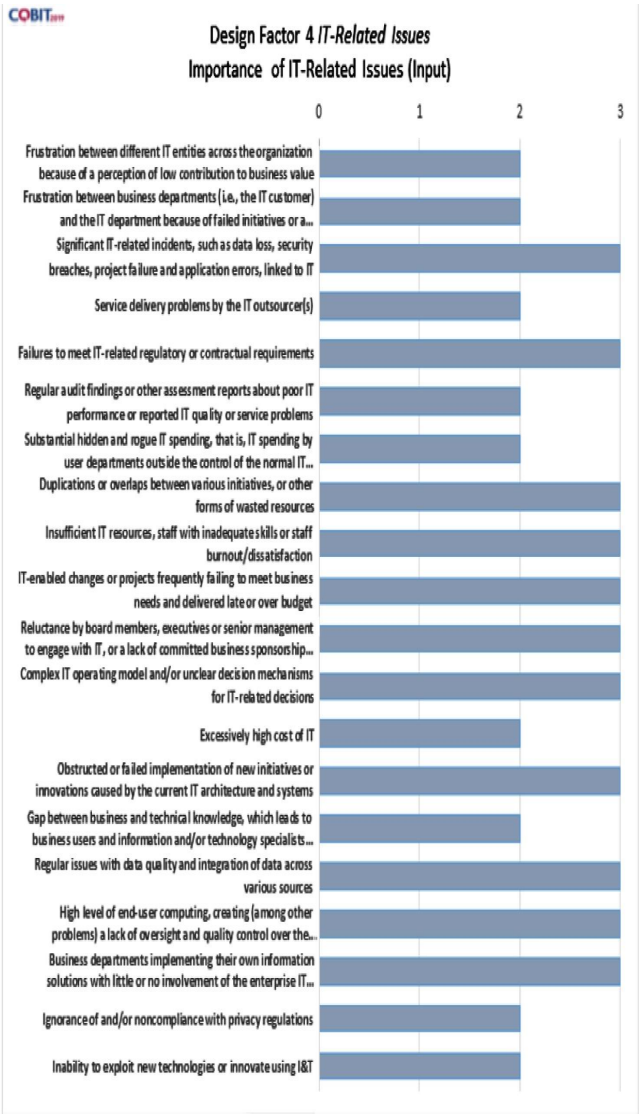

Fig. 8. Design factor assessment of IT-related issues.

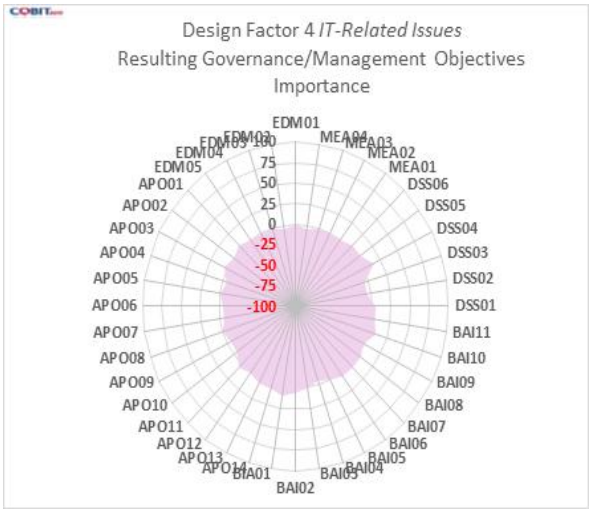

Fig. 9. IT governance areas/domains related to DF 04.

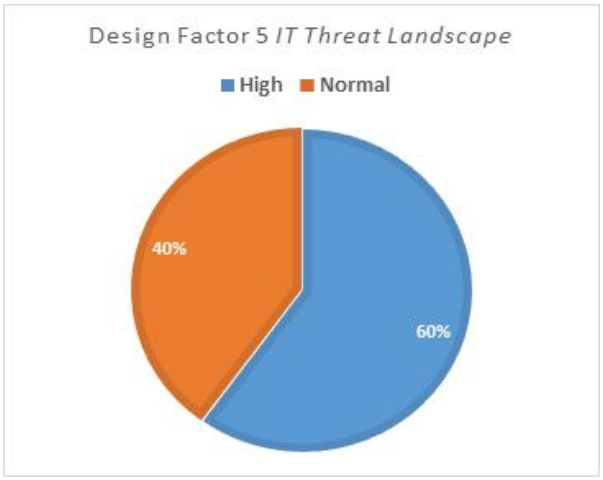

Fig. 10. Design Factor Threat Landscape Value

In the figure 11, we can see the assessment results show that many domains or areas need to be addressed in governance related to threats. There are 23 domains or areas that require focus to achieve Pustipanda's objective of managing high-impact threats.

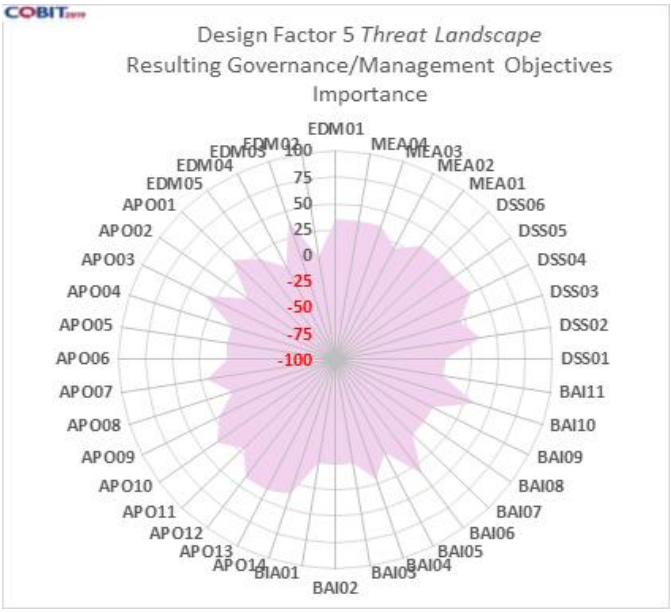

Fig. 11. Area/domain of IT governance related to DF 05.

F. Compliance Requirements

For this design factor, there are three assessment levels: low compliance requirement, medium compliance requirement, and high compliance requirement (Fig. 12). Pustipanda's assessment shows that 11% of compliance requirements have a low priority, 33% have a medium priority, and 56% have a high priority. This indicates that Pustipanda must adhere to a set of regulatory compliance requirements that are above average, given that 56% fall into the high-priority category.

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 111–120
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.45011
©2025. The Author(s). This is an open acces article under cc-by-sa

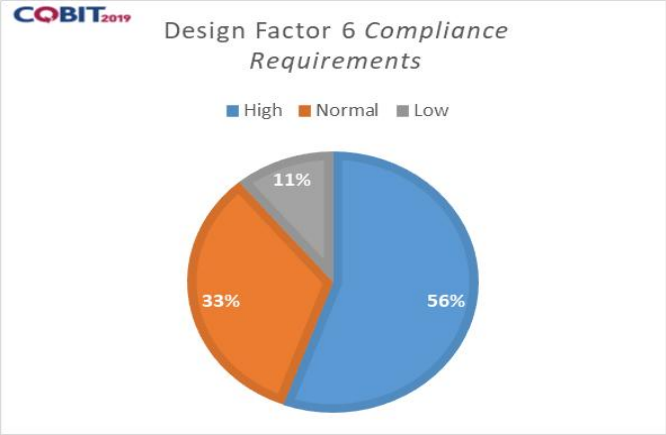

Fig. 12. Design factor 6 compliance requirements.

In the Fig. 13, we can see this affects the prioritization of several related domains, including EDM 01, EDM 03, EDM 05, APO 10, APO 12, APO 13, DSS 04, DSS 05, MEA 03, and MEA 04.

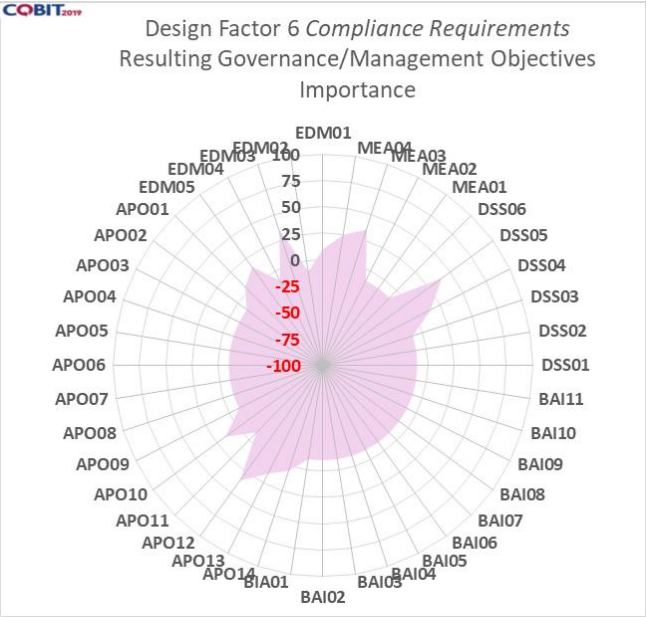

Fig. 13. IT governance areas/domains related to DF 06.

G. Role of IT

The role of IT in an organization or company is classified into four categories: Support, Factory, Turnaround, and Strategic (Fig. 14). The highest score was given to IT's strategic role. Pustipanda's assessment of the role of IT at UIN Syarif Hidayatullah can be seen in figure 15. The highest value is given to the strategic role of IT, so that from this assessment the priority of the related domains is APO 04.

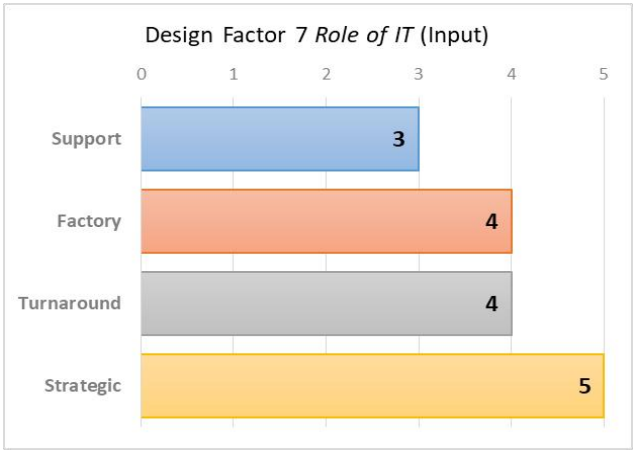

Fig. 14. Design factor assessment role of IT.

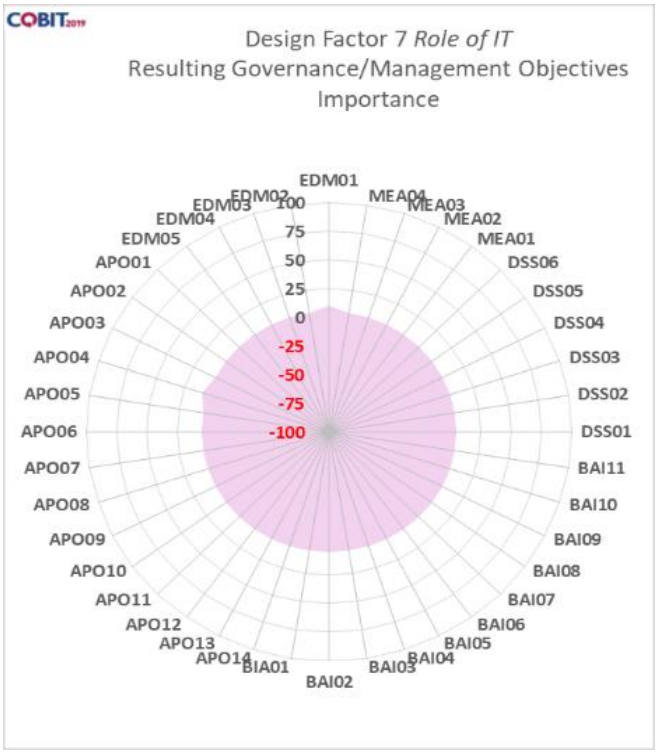

Fig. 15. IT governance areas/domains related to DF 07.

H. Sourcing Model of IT

An organization's IT procurement model can be categorized into three types: outsourcing, cloud, and insourcing. The choice of procurement model impacts various aspects such as human resources and financial management (Figure 16). Pustipanda predominantly uses the insourced model, which requires a solid and reliable IT team to manage the technology.

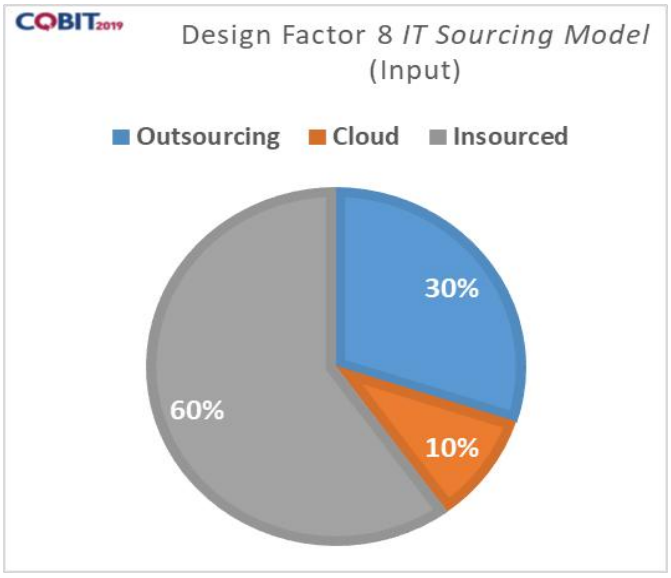

Fig. 16. IT sourcing model design factor assessment.

In the Fig. 17, we can see this decision determines the priority domains related to IT governance, namely EDM 03, APO 09, APO 10, APO 12, and MEA 01.

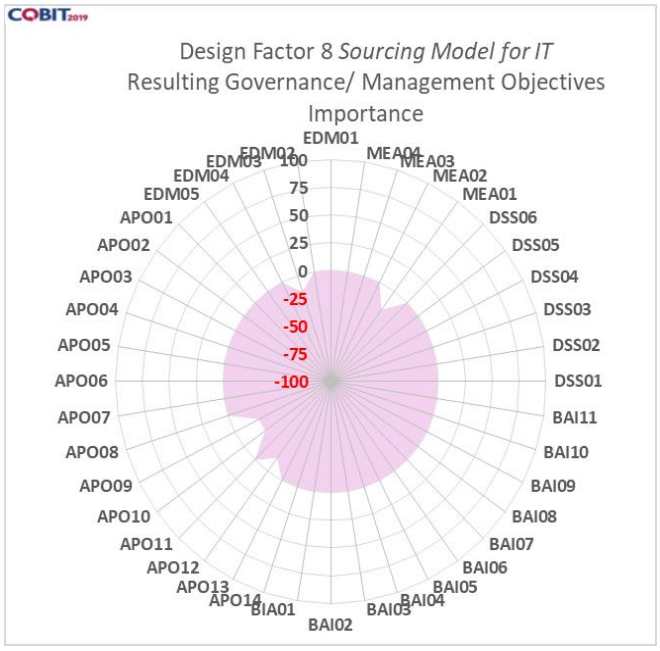

Fig. 17. IT governance areas/domains related to DF 08.

I. IT Implementation Methods

There are three IT implementation methods: Agile, DevOps, and Traditional. Pustipanda primarily uses the Traditional implementation method, accounting for 80% of its IT implementations (Fig. 18).

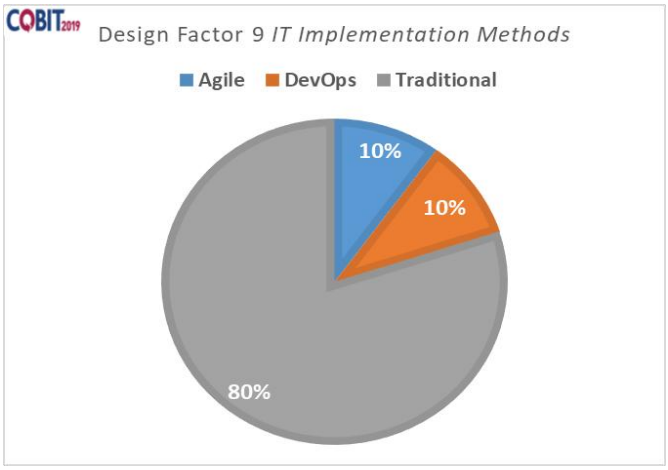

Fig. 18. Design factor assessment IT.

Consequently, the priority IT governance domains related to this approach are BAI 01, BAI 02, BAI 03, BAI 05, BAI 06, BAI 07, and BAI 11 (figure 19). This shows that nearly all BAI domains require attention from Pustipanda.

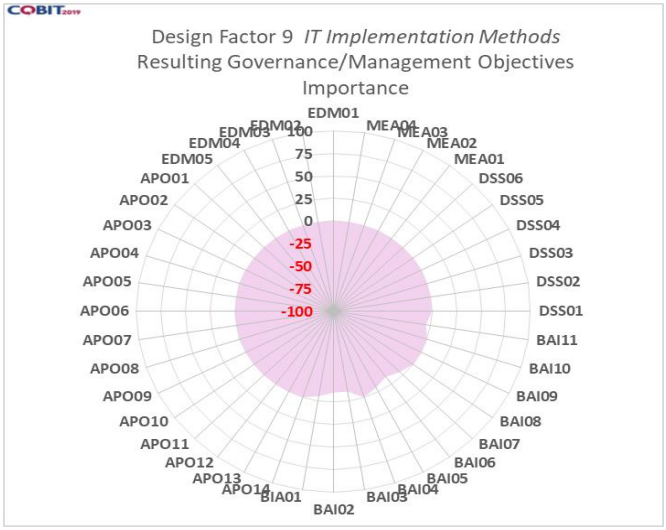

Fig. 19. IT governance areas/domains related to DF 09.

J. Technology Adoption Strategy

Based on the assessment of this design factor, the highest score was given to the "slow adopter" category (Fig. 20). This indicates that Pustipanda experiences challenges in IT development, which in turn affects the achievement of organizational goals.

Applied Information System and Management (AISM)
Volume 8, (1) 2025, p. 111–120
P-ISSN: 2621-2536; E-ISSN: 2621-2544; DOI: 10.15408/aism.v8i1.45011
©2025. The Author(s). This is an open acces article under cc-by-sa

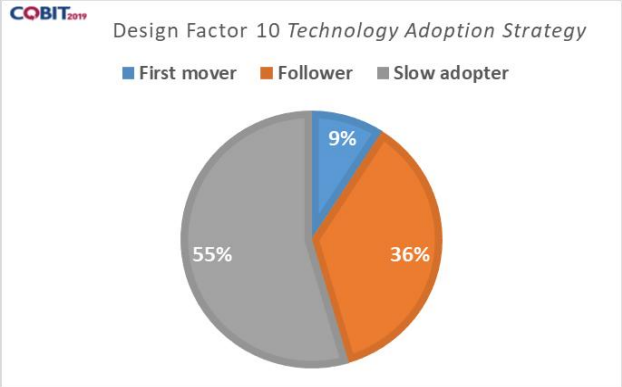

Fig. 20. Design factor assessment technology adoption strategy.

If we look at Fig. 21, there are 25 domains or areas that are needed.

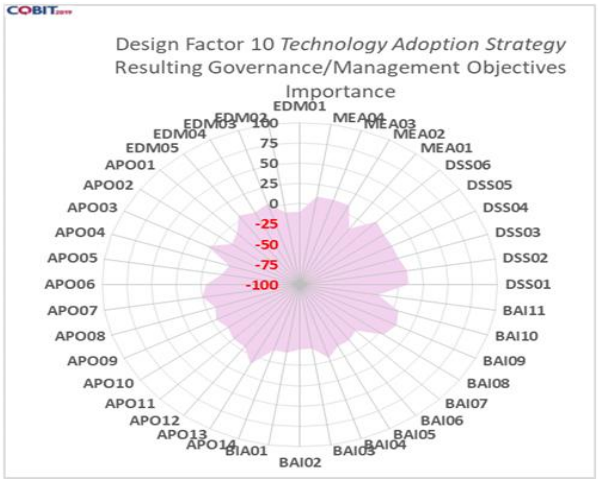

Fig. 21. IT governance areas/domains related to DF 10.

K. Company/Organization Size

UIN Syarif Hidayatullah is a large PTKIN (State Islamic University) with thousands of students, as well as a significant number of faculty members and staff. The large size of the organization necessitates robust IT governance to ensure that the university's objectives are successfully achieved.

I. IT Governance Design Result

The processes deemed essential are those exhibiting the highest capability level, specifically level 4 with a score of 75, as illustrated in Fig. 21. This figure delineates 40 processes, each with varying weights attributed to the input values from design factors 1 through 11. These values range from 100 to -55, where positive values indicate the significance of a governance process to the organization, while negative values suggest a process's non-core status. Based on Figure 21, it is evident that among the 40 core model or critical IT processes at Pustipanda, those scoring above 75% are prioritized. These include: 1) EDM03-Ensure Risk Optimization, 2) APO13-Manage Security, 3) DSS04 - Manage Continuity, 4) DSS05 - Manage Security Services, 5) MEA03 - Manage Compliance with External Requirements, and 6) MEA04 - Manage Assurance

The analysis highlights several key IT governance processes, each achieving a target capability level of 4. Notably, EDM03–Ensure Risk Optimization, with a score of 90, focuses on the optimal identification, analysis, and management of IT risks to support business objectives. Similarly, DSS04–Manage Continuity, also scoring 90, ensures the continuous accessibility of academic systems, even during incidents like server crashes. APO13–Manage Security, scoring 85, emphasizes the importance of setting security policies for the development and use of academic systems, protecting sensitive student data, and mitigating cyberattack risks. DSS05–Manage Security Services, achieving a perfect score of 100, underscores the necessity of providing active security features like firewalls, anti-malware, and suspicious activity detection for academic systems. MEA03–Manage Compliance with External Requirements, scoring 95, ensures that academic systems adhere to personal data protection regulations. Finally, MEA04–Manage Assurance, with a score of 75, involves conducting regular audits and assessments of academic information systems to guarantee quality, security, and effectiveness, while also facilitating performance reporting to campus management or clients. Each of these processes plays a critical role in maintaining robust and effective IT governance within the academic environment.

V. CONCLUSION

The conclusion of this study is that by assessing the design factors of IT governance using COBIT 2019, organizations can determine the priority scale of the 40 domains within IT governance based on the COBIT 2019 framework. This enables organizations to implement governance according to their specific needs. The research findings indicate that UIN Syarif Hidayatullah has 22 priority domains for implementation. Based on the 11 design factors, only 22 domains are prioritized, namely EDM01 (Ensure Governance Framework Setting and Maintenance), EDM03 (Ensure Risk Optimization), EDM05 (Ensure Stakeholder Engagement), APO01 (Manage the IT Management Framework), APO03 (Manage Enterprise Architecture), APO08 (Manage Relationships), APO11 (Manage Quality), APO12 (Manage Risk), APO13 (Manage Security), APO14 (Manage Data), BAI06 (Manage IT Changes), BAI08 (Manage Knowledge), BAI10 (Manage Configuration), DSS01 (Manage Operations), DSS02 (Manage Service Requests and Incidents), DSS03 (Manage Problems), DSS04 (Manage Continuity), DSS05 (Manage Security Services), DSS06 (Manage Business Process Controls), MEA02 (Monitor, Evaluate, and Assess the System of Internal Control), MEA03 (Monitor, Evaluate, and Assess Compliance with External Requirements), and MEA04 (Monitor, Evaluate, and Assess IT Governance). Additionally, there are two domains that are not considered at all in IT governance, which

are APO10 (Manage Suppliers) and MEA01 (Monitor, Evaluate, and Assess Performance and Conformance). This method can be adopted by other PTKIN institutions to determine the priority scale of domains in IT governance.

This study is subject to certain limitations. First, it focuses solely on determining the priority domains of IT governance based on design factors and does not cover the actual implementation of the governance. Second, the study does not delve deeply into the practical steps required to implement the recommended governance model, including the challenges and obstacles that may arise during the implementation process. Third, this research does not extend to the calculation of capability levels. Therefore, the findings of this study should be interpreted within these limitations.

The recommendation from this study is that once the priority scale of IT governance domains has been identified, Pustipanda can develop IT governance based on the priorities obtained from the design factor assessment. Future research can focus on further developing IT governance based on these priorities, particularly concerning risk management. Furthermore, the risk analysis model can be further developed by referring to other risk management frameworks, such as OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

ACKNOWLEDGMENT

The author would like to express gratitude to Prof. Dr. Amany Lubis, MA, Rector of Syarif Hidayatullah State Islamic University Jakarta. Special thanks also go to Dr. Imam Subchi, MA, Head of the Research and Publication Center (PUSLITPEN) at Syarif Hidayatullah State Islamic University Jakarta. Lastly, appreciation is extended to the ITIDOP Research Group of the Information Systems Department at Syarif Hidayatullah State Islamic University Jakarta for their support of this research.

REFERENCES

[1] J. S. Suroso and M. Fakhrozi, "Assessment of information system risk management with Octave Allegro at system education," *Procedia Comput. Sci*., vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[2] M. Moyo, H. Abdullah, and R. C. Nienaber, "Information security risk management in small-scale organizations: A case study of secondary schools computerized information systems," *2013 Information Security for South Africa, Johannesburg, South Africa*, pp. 1–6, 2013, doi: 10.1109/ISSA.2013.6641062.

[3] B. M. Dioubate, N. N. Molok, S. Talib, and A. O. Trap, "Risk assessment model for organizational information security," *ARPN J. Eng. Appl. Sci*., vol. 30, no. 23, pp. 17607–17613, 2015.

[4] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur*., vol. 44, pp. 1–15, 2014, doi: 10.1016/j.cose.2014.04.005.

[5] M. Talabis and J. Martin, *Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis*. Newnes, 2012.

[6] A. T. D. Aryani, R. Ahmad, and P. Bill, "User satisfaction on academic information system in UIN KH abdurrahman wahid pekalongan," *Appl. Inf. Syst. Manag.*, vol. 6, no. 2, pp. 97–104, 2023, doi: 10.15408/aism.v6i2.31245.

[7] K. C. Laudon and J. P. Laudon, *Management Information System,* thirteenth edition. Pearson, 2004.

[8] H. Alves and M. Raposo, "The influence of university image on student behaviour," *Int. J. Educ. Manag*., vol. 24, no. 1, pp. 73–85, 2010, doi: 10.1108/09513541011013060.

[9] I. Sherifi, "Impact of information systems in satisfying students of the university: Case study from epoka university," *Eur. J. Bus. Soc. Sci.,* vol. 4, no. 04, pp. 167–175, 2015.

[10] H. A. Salsabila and I. Iriyadi, "Evaluasi atas penerapan sistem informasi akademik dan keuangan terhadap tingkat kepuasan mahasiswa (studi kasus mahasiswa jurusan akuntansi S1 angkatan tahun 2016 di IBI kesatuan bogor)," *J. Anal. Sist.* Pendidik. Tinggi, vol. 4, no. 2, pp. 137–148, 2020, doi:10.36339/jaspt.v4i2.348.

[11] N. L. Kuntari, Y. H. Chrisnanto, and A. I. Hadiana, "Manajemen risiko sistem informasi di Universitas Jenderal Achmad Yani menggunakan metoda OCTAVE Allegro," *in Seminar Nasional Teknologi Informasi*, vol. 1, pp. 551-559, Jul. 2018.

[12] D. A. Jakaria, R. T. Dirgahayu, and H. Hendrik, "Manajemen risiko sistem informasi akademik pada perguruan tinggi menggunakan metoda Octave Allegro," *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, pp. 37–42, 2013.

[13] M. I. Cholik, "Analisis manajemen risiko penggunaan sistem informasi menggunakan metode octave allegro (studi kasus PT. XYZ)," M.S. Thesis, Bina Nusantara University, 2018

[14] A. Safar, "Deteksi penilaian resiko pada e-learning SMK bina prestasi AMI balikpapan dengan metode octave allegro," *J. Sist. Inf*., vol. 2, no. 2, pp. 69–77, 2019.

[15] R. Rosini, M. Rachmaniah, and B. Mustafa, "Penilaian risiko kerawanan informasi dengan menggunakan metode octave allegro," *J. Pustakawan Indones*., vol. 14, no. 1, pp. 1–9, 2015.

[16] A. Zulfia, E. L. Ruskan, and P. Putra, "Penilaian risiko aset informasi dengan metode octave allegro: Studi kasus ICT fakultas ilmu komputer Universitas Sriwijaya," *J. Inf. Syst*., vol. 6, no. 1, pp. 40–47, 2021, doi: 10.33633/joins.v6i1.4088.

[17] M. G. Ginanjar, L. Ramadhan, and R. A. Nugraha, "Perancangan tata kelola teknologi informasi menggunakan kerangka kerja COBIT 2019 di DISKOMINFOSAN kabupaten sukabumi," *Smart Comp*, vol. 10, no. 03, pp. 160–165, 2021.

[18] P. N. Anastasia and L. H. Atrinawati, "Perancangan tata kelola teknologi informasi menggunakan *framework* cobit 2019 pada hotel xyz," *JSI J. Sist. Inf*., vol. 12, no. 2, pp. 2088–2099, 2020, doi: 10.36706/jsi.v12i2.12329.

[19] L. Merryana, I. Ade, & H. Hendry, "Information technology governance design in devops-based e-marketplace companies using COBIT 2019 framework" *INTENSIF,* vol. 6, no. 2, pp. 233–252, 2022, doi: 10.29407/intensif.v6i2.18104.

[20] J. Beato, and M. I. Fianty, "COBIT 2019 framework: Evaluating knowledge and quality management capabilities in a printing machine distributor" *Journal of Information Systems and Informatics*, vol. 6, no. 1, pp. 1–12, 2019, doi: 10.51519/journalisi.v6i1.638.