[1] Kathryn P. Acosta

[2]Thelma D. Palaoag

Synergizing IoT-Based Gender-Responsive Security Surveillance to Gauge ICT Infrastructure Maturity

JES Journal of Electrical Systems

Abstract: - Effective planning and implementation of smart security surveillance ensures campus protection for all genders. Thus, the integration of a reliable ICT infrastructure as the core foundation for the security and privacy of the institutions leads to a substantial transformation in the way individuals interact, increasing the confidentiality of the stakeholders. Hence, the study aims to assess the current state of ICT infrastructure and identify the parameters in the design of an IoT-based gender-responsive security surveillance system for Colegio de San Juan de Letran Manaoag. The study implemented a comprehensive review of related literature about maturity models and their capabilities. A focus group discussion was assembled to administer a semi-structured interview on the current state of the ICT infrastructure and conducted an online survey for the assessment of the ICT infrastructure among the administrators and staff of the MIS Department in identifying the strengths and weaknesses of the current ICT infrastructure. Employing the IT Infrastructure Maturity Model (ITI-MM) as a tool in determining the maturity levels of its capabilities. Based on the results, the ITI-MM model determined the current state of the ICT infrastructure, which is currently operating at maturity level 2, and identified the gaps in achieving the requirements between Level 1 and Level 2. In conclusion, the study indicated that measuring of the maturity level is applicable in integrating the proposed system for developing an IoT-based gender-responsive security surveillance system to enhance the security measures of the institution.

Keywords: Gender-Responsive, Internet of Things (IoT), ICT Infrastructure, Security, Maturity Model

I. INTRODUCTION

In schools, safety and security of all genders are significant concerns, and one of the important aspects is innovation in intelligent security surveillance. Hence, following high-profile instances of violence in schools, school administrators have become more dependent on a variety of surveillance techniques to ensure authority and discipline in their educational institutions[1]. Some individuals view a campus as a location for comfort, security, sustainability, recreation, and learning, enhanced by a variety of cutting-edge systems and technologies[2][3]. Utilizing the internet of things is inevitable, as it forms a core component of the smart campus[4]. The widespread adoption of the Internet of Things (IoT) has sparked a revolutionary transformation across all aspects of life[5]. In addition, the Internet of Things (IoT) is widely recognized as one of the most important areas of emerging technology, attracting considerable attention from different organizations[6]. With the integration of these technologies, methods of discipline, assessment, and supervision within school populations have progressively grown, often with comparatively less controversy and opposition than the application of surveillance technologies in broader society[7]. Hence, to address the violence, certain schools are adopting sophisticated artificial intelligence surveillance technology, incorporating facial recognition and geolocation tracking devices, as a means to enhance security measures[8]. Enhanced surveillance in public spaces serves as a significant deterrent against delinquent behavior, creating a safer environment for everyone involved[9][10][11].

Thus, Colegio de San Juan de Letran Manaoag seeks to ensure that the environment is safe and secure for teaching and learning. The present challenge is how, with the current ICT infrastructure available, to successfully identify the incidences of bullying, sexual assault, sexual harassment, and other crimes utilizing video surveillance that undermine gender responsiveness in a campus setting. Information and communication technology is now considered a crucial element in educational institutions[12] Furthermore, ICT maturity models are gaining popularity in service science as they are employed to facilitate continuous improvement and

[1] College of Information Technology and Computer Science University of the Cordilleras Baguio City, Philippines
kathyacosta2019@gmail.com

[2]College of Information Technology and Computer Science University of the Cordilleras Baguio City, Philippines
tdpalaoag@uc-bcf.edu.ph

evaluate service organizations through self or third-party assessments[13][14]. According to [15], a maturity model is a method that has been shown to be useful in evaluating several facets of the procedures of an organization. The term maturity can be defined as the distinct levels of development that characterize a particular entity or dimension[16][17]. In this context, a maturity model serves as a framework or guide that enables a clearer comprehension of reality, and its primary objective is to explain a particular phenomenon and empower the ability to make predictions based on the insights gained from the model[18]. The maturity model enables the organization to comprehend processes better, establish standard measurements, and facilitate the implementation of potential enhancements[19].

Hence, the study aims to assess the current state of the ICT infrastructure and identify the parameters using the maturity model in the design of an IoT-based gender-responsive security surveillance system for Colegio de San Juan de Letran Manaoag. Enhancing the ICT infrastructure and effectively addressing and preventing gender-based violence, harassment, and discrimination necessitates overcoming the current system's limitations in identifying intruders, gender-based violence, or suspicious activity across all genders. Given these issues, it is important to scrutinize whether the current real-time video surveillance system can be enhanced to provide a more effective safety solution for the Colegio.

II. METHODOLOGY

A comprehensive review of related literature about the different infrastructure maturity models and their capabilities. Additionally, this review focuses on analyzing the key influencing factors or dimensions as well as the assessment tools, which serve as the primary criteria for evaluation. The comprehensive synthesis of findings from multiple studies on infrastructure maturity models asserts that organizations need to fulfill all the goals of process areas from a specific perspective, as determined by the assessment tools in use, in order to attain a higher capability or maturity level. In the data collection, a focus group discussion was administered through a semi-structured interview on the current state of the ICT infrastructure. The study conducted an online survey for the assessment of the current ICT infrastructure using the ITI-MM tool, a comprehensive and accurate assessment of the current ICT infrastructure maturity level. The IT Infrastructure Maturity Model (ITI-MM) method adopted in the assessment of the ICT infrastructure proved to be the most appropriate and effective tool for determining its maturity level. Through the use of the ITI-MM assessment tool[20], as depicted in Fig. 1 which consist of domains, levels, capabilities, and perspectives in assessing the criteria that are currently used by the institutions regarding ICT infrastructure. After a thorough review of related literature, a comparative analysis was used to analyze the criteria of the different IT infrastructure maturity models. Through a descriptive analysis to describe the current ICT infrastructure among the administrators and MIS Department staff. Using comparative analysis on the ITI-MM assessment maturity tool to measure the maturity level of the existing ICT infrastructure of the institution and determine the gaps between Level 1 and Level 2 assessments.

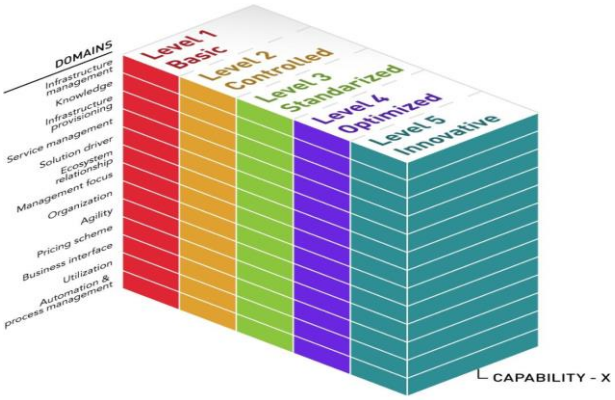

Fig. 1. The ITI-MM Model.

III. RESULTS AND DISCUSSIONS

Given that there are commonalities among the eight (8) maturity models analyzed, the ITI-MM is well-suited for the assessment of the ICT infrastructure as illustrated in Table I. The ITI-MM has significant implications for enterprise architecture and IT governance as well.

TABLE I. COMPARATIVE ANALYSIS ON MATURITY MODELS

Maturity model	**Influencing Factors / Dimensions**	**Assessment Tool**	**References**
Capability Maturity Model Integration (CMMI)	IT Governance Service, Product, and SW Development	Technology Infrastructure Tools and Services, CMMI Questionnaires, and Gap Analysis	[21][22][23] [24][25]
Autonomic Maturity Level	Self-Configuration, Self-Optimization, Self-healing, Self-protection	Self-Assessment Questionnaires and Define the Maturity Model	[26]
IT Infrastructure Library (ITIL)	Service Life Cycle Approach Service Level Agreements (SLAs)	Self-Assessment Questionnaires, Define the Maturity Model, and ITIL Tools	[27][28]
Green Maturity Model for Virtualization	Resource Utilization	Virtualization Performance Monitoring, Benchmarking and Define the Maturity Model	[29][30]
COBIT 5	IT Governance and Business Process	Process Assessment Management (PAM), Define the Maturity Model, and Gap Analysis	[31] [32][33]
Gartner Infrastructure Maturity Model (GIMM)	Technology Infrastructure, IT Service Management (ITSM)	Define the Maturity Model, Customized Maturity Model Self-Assessment Questionnaires, Gap Analysis, and Gartner IT Score – IT Maturity Assessment	[34][35][36]

NHS Infrastructure Maturity Model (NIMM)	Technology Stack	KPIs, Critical Success Factors, Best Practice, Standards, Patterns, and Practices, and Define the Maturity Model	[37][38] [39]
IT Infrastructure Maturity Model (ITI-MM)	IT Governance and Enterprise Architecture, Low Cost, Scalability, Flexibility, and Agility	Define the Maturity Model, Key Dimension, Self- Assessment, Create Assessment Criteria, Scoring Mechanism, Data Collection, Assessment Execution, Continuous Improvement, Validation, and Gap Analysis	[20][40]

Based on the comprehensive review of related literature, the assessment tool that is more applicable in the assessment of the ICT infrastructure was the ITI-MM because of its efficiency, low cost, agility, and easy-to-find ICT infrastructure performance indicator, which is needed in the study.

Moreover, the respondents assessed their ICT infrastructure by scoring each capability from one (1) to five (5), using one or more perspectives to help them shape their ways of thinking. After completing the assessment session, respondents are required to utilize the provided numbers and lines of reasoning as argumentation to determine the rational maturity score for each capability. It is essential to note that each capability can only have a single maturity score. Applying the five (5) ITI-MM views to evaluate the capacity holistically, the ICT infrastructure capabilities that are acquired from the scores and lines of reasoning derived from each perspective are then utilized as argumentation to arrive at the final maturity level for a capability.

TABLE II. ITI-MM LEVEL 1 ASSESSMENT

Domain	**Perspectives/ Capabilities**	**Assessment**	**Remarks**
Infrastructure Management	Infrastructure Storage Platform Server Management Capability	The server enables the availability of shared resources, internet connectivity, and NAS functionalit	LEVEL 1 ACHIEVED

		y.	
Agility	Procurement Strategy Capability	Making preparations in advance to guarantee timely, cost-effective, as-needed acquisition of the products and services that the organization requires to function.	LEVEL 1 ACHIEVED
Knowledge	People and Skills IT Staff Training Capability	Provided training and seminars to upgrade the knowledge and skills of IT staff.	LEVEL 1 ACHIEVED
Knowledge	People and Skills IT Staff Performance Capability	IT staff performance management is present.	LEVEL 1 ACHIEVED
Infrastructure Provisioning	IT Security and Information Governance Surveillance System Capability	Analog and IP cameras on the current surveillance system are in place for monitoring and keeping track of the activities at the school.	LEVEL 1 ACHIEVED
Infrastructure Provisioning	End User Devices Email Capability	Provide a new email account to students, administration, faculty, and staff of	LEVEL 1 ACHIEVED

		the school.	
Infrastructure Management	Process and Automation Infrastructure Processes Documentation Capability	There is efficiency, productivity, cost savings, compliance, reduced errors, and increased employee satisfaction and retention.	LEVEL 1 ACHIEVED
Infrastructure Management	IT Security and Information Governance Data Security Capability	Safeguarding sensitive information from unauthorized access and misuse and reducing the risk of data breaches are present.	LEVEL 1 ACHIEVED

The ITI-MM Level 1 and Level 2 assessments were based on the focus group discussion of the participants using the ITI-MM assessment tool, which determined the strengths and weaknesses as well as the recommendations for improving the current ICT infrastructure in the institution. As shown in Table. II, the ITI-MM Level 1 Assessment results, the infrastructure management domain capabilities in the context of infrastructure storage platform server management capability, and the server successfully fulfilling the criteria by providing access to shared resources, internet connectivity, and NAS functionality of Level 1 based on the assessment of the respondents. In addition, in the agility domain that has procurement strategy capability, preparation of the organization in advance is apparent regarding the guarantee of meeting the requirements, which are available and functional and defined as Level 1. Meanwhile, the knowledge domain people and skills IT staff training capability, trainings, and seminars are provided to upgrade the knowledge and skills of IT staff that satisfy the criteria in Level 1. Moreover, Level 1 was also achieved in the knowledge domain of people and skills for IT staff performance capability, where IT staff performance management is present. Additionally, the infrastructure provisioning has IT security and information governance capabilities, and the surveillance system capability encompasses both analog and IP cameras, effectively monitoring and recording school activities. This has satisfied the requirements of Level 1. Furthermore, the infrastructure provisioning domain, which consists of end-user device email capability and provides new email to the students, administration, faculty, and staff, adhered to level 1. Meanwhile, Level 1 was achieved in process and automation infrastructure processes documentation capability. Having an effective, efficient system leads to productivity gains, cost savings, compliance, fewer errors, heightened employee satisfaction, and improved retention. Subsequently, the infrastructure management domain in IT security and information governance data security capability has met the requirements in Level 1.

TABLE III. ITI-MM LEVEL 2 ASSESSMENT

Domain	Perspectives/ Capabilities	Assessment	Remarks
Infrastructure Management	Infrastructure Storage Platform Server Management Capability	There is network security in place, such as the Fortinet Firewall.	LEVEL 2 ACHIEVED
Agility	Procurement Strategy Capability	The procedure for tracking the supplier is fast and efficient.	LEVEL 2 ACHIEVED
Knowledge	People and Skills IT Staff Training Capability	Consistently enacting an all-encompassing training program for the IT staff.	LEVEL 2 ACHIEVED
Knowledge	People and Skills IT Staff Performance Capability	There is a need to enhance skills and expertise through IT certifications.	LEVEL 2 NOT ACHIEVED
Infrastructure Provisioning	IT Security and Information Governance Surveillance System Capability	The current surveillance system cannot identify intruders in real time, and there are no existing notifications.	LEVEL 2 NOT ACHIEVED
Infrastructure Provisioning	End User Devices Email Capability	There is an established and standardized email provisioning process across all	LEVEL 2 ACHIEVED

		accounts.	
Infrastructure Management	Process Automation Infrastructure Processes Documentation Capability	A paperless system is to be implemented.	LEVEL 2 NOT ACHIEVED
Infrastructure Management	Common Application and Services End User Devices Email Capability	A firewall filtering measure is present.	LEVEL 2 ACHIEVED

As shown in Table III, the results of the ITI-MM Level 2 Assessment from the respondents indicate capabilities in infrastructure management on infrastructure storage platforms and server management. Network security measures, including the utilization of the Fortinet firewall that adheres to Level 2 requirements, have been implemented. Moreover, in the agility domain, which consists of the procurement strategy capability, the procedure for tracking the supplier is fast and efficient. Level 2 criteria were attained. In addition, knowledge comprising the people and skills IT staff training capability and maintaining a continual and comprehensive training initiative for the IT staff, Level 2, was obtained. Furthermore, because the knowledge domain consisting of the people and skills required for IT staff performance capability, Level 2, was not attained, it is necessary to elevate skills and expertise via IT certifications. Moreover, in the domain of infrastructure provisioning within IT security and information governance surveillance systems, the existing surveillance system lacks the capability to promptly detect intruders and lacks any notifications in place, thus preventing it from reaching the necessary level 2. On the other hand, in the infrastructure provisioning domain consisting of end-user device email capability, an email provisioning process has been implemented and standardized across all accounts that meet the requirements in Level 2. Furthermore, due to the upcoming implementation of a paperless system, the infrastructure management on process automation infrastructure processes documentation capability did not reach Level 2. Moreover, the infrastructure management consisting of the common applications and services and end-user device email capability has obtained Level 2, since firewall filtering measures are present. The level of maturity based on the results of the domains, capabilities, and perspectives is at Level 2 (controlled). The typical incentive for progressing to this stage arises from a desire to attain a more enhanced and uniform perspective of the current infrastructure, coupled with a drive to assume greater command and authority.

IV. CONCLUSION

In conclusion, measuring the ICT infrastructure using the ITI-Maturity Model is also the most appropriate tool to use in determining the different capabilities of the domains in the current ICT infrastructure of the institution. The ITI-MM assessment through focus group discussion helped the school determine the current ICT infrastructure of Colegio de San Juan de Letran Manaoag. The ITI-MM model determined the current state of the ICT infrastructure and identified the gaps in achieving the requirements between Level 1 and Level 2. The researchers also found out that the identified parameters using the ITI-MM are significant to integrate into the proposed system.

Furthermore, the maturity level in the domains, capabilities, and perspectives indicates that the current ICT infrastructure is applicable for developing a proposed system for an IoT-based gender-responsive security surveillance system to enhance the security measures of the institution.

REFERENCES

[1] J. P. Nance, "Student Surveillance, Racial Inequalities, and Implicit Racial Bias," *Emory Law J.*, vol. 66, no. 4, pp. 765–837, 2016, [Online]. Available: http://www.ed.gov/news/press-releases/new-data-us-department-education-

[2] K. Polin, T. Yigitcanlar, M. Limb, and T. Washington, "The Making of Smart Campus: A Review and Conceptual Framework," *Buildings*, vol. 13, no. 4, 2023, doi: 10.3390/buildings13040891.

[3] M. Gao, "Smart campus teaching system based on ZigBee wireless sensor network," *Alexandria Eng. J.*, vol. 61, no. 4, pp. 2625–2635, 2022, doi: 10.1016/j.aej.2021.09.001.

[4] A. Abdullah, M. Thanoon, and A. Alsulami, "Toward a smart campus using IoT: Framework for safety and security system on a university campus," *Adv. Sci. Technol. Eng. Syst.*, vol. 4, no. 5, pp. 97–103, 2019, doi: 10.25046/aj040512.

[5] H. Afreen, M. Kashif, Q. Shaheen, Y. H. Alfaifi, and M. Ayaz, "IoT-Based Smart Surveillance System for High-Security Areas," *Appl. Sci.*, vol. 13, no. 15, 2023, doi: 10.3390/app13158936.

[6] A. F. Santamaria, P. Raimondo, M. Tropea, F. De Rango, and C. Aiello, "An IoT surveillance system based on a decentralised architecture," *Sensors (Switzerland)*, vol. 19, no. 6, 2019, doi: 10.3390/s19061469.

[7] S. Nemorin, "Nemorin Selena Post-panoptic pedagogies: the changing nature of school surveillance in the digital age Article (Accepted version) (Refereed) under a Creative Commons BY-NC-ND 4.0 license: https://creativecommons.org/licenses/by-nc-nd/4.0," no. July, 2017.

[8] M. Weinstein, "School of Surveillance: The Students' Rights Implications of Artificial Intelligence as K-12 Public School Security," *NCL Rev.*, vol. 98, no. 2, 2019, [Online]. Available: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nclr98&section=22%0Ahttps://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=6772&context=nclr

[9] T. Anagnostopoulos *et al.*, "Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey," *IEEE Access*, vol. 9, pp. 131926–131954, 2021, doi: 10.1109/ACCESS.2021.3114447.

[10] L. Wang, C. Yao, Y. Yang, and X. Yu, "Research on a Dynamic Virus Propagation Model to Improve Smart Campus Security," *IEEE Access*, vol. 6, pp. 20663–20672, 2018, doi: 10.1109/ACCESS.2018.2817508.

[11] J. Mullins, "Ring of steel II: New york city gets set to replicate london's high-security zone," *IEEE Spectr.*, vol. 43, no. 7, pp. 12–13, 2006, doi: 10.1109/MSPEC.2006.1652996.

[12] T. B. Ntorukiri, F. Kirimi Kiara, and M. Celestino, "Impact of Integrating ICT Infrastructure in Teaching and Learning in Kenyan Secondary Schools in Meru County," *Eur. Acad. Res.*, vol. VIII, no. 12/March 2021, 2021, [Online]. Available: www.euacademic.org

[13] G. O. Ekuobase and V. A. Olutayo, "Study of Information and Communication Technology (ICT) maturity and value: The relationship," *Egypt. Informatics J.*, vol. 17, no. 3, pp. 239–249, 2016, doi: 10.1016/j.eij.2015.12.001.

[14] I. Boughzala and I. Bououd, "A community maturity model: An application for assessing knowledge sharing in the field," *PACIS 2011 - 15th Pacific Asia Conf. Inf. Syst. Qual. Res. Pacific*, 2011.

[15] D. Proença and J. Borbinha, "Maturity Models for Information Systems - A State of the Art," *Procedia Comput. Sci.*, vol. 100, no. June 2017, pp. 1042–1049, 2016, doi: 10.1016/j.procs.2016.09.279.

[16] E. Boström and O. C. Celik, "Appendix A: The Maturity Model of Digital Strategizing (MMDS) Department of informatics IT Management Master thesis 2-year level Towards a Maturity Model for Digital Strategizing A qualitative study of how an organization can analyze and assess their digi," *Inform. Student Pap. Master NV - SPM 2017.09*, pp. 30–2017, 2017, [Online]. Available: http://umu.diva-portal.org/smash/get/diva2:1113444/FULLTEXT01.pdf%0Ahttp://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-136736

[17] K. V. Andersen and H. Z. Henriksen, "E-government maturity models: Extension of the Layne and Lee model," *Gov. Inf. Q.*, vol. 23, no. 2, pp. 236–248, 2006, doi: 10.1016/j.giq.2005.11.008.

[18] E. Tocto-Cano, S. P. Collado, J. L. López-Gonzales, and J. E. Turpo-Chaparro, "A systematic review of the application of maturity models in universities," *Inf.*, vol. 11, no. 10, pp. 1–15, 2020, doi:

10.3390/info11100466.

[19] T. Andjarwati, A. Hermanto, and . S., "Gap Analysis and Measurement of Information Technology Readiness for Improvement of Competitive Capabilities to Small and Medium Enterprises in East Java," *KnE Soc. Sci.*, vol. 3, no. 10, p. 12, 2018, doi: 10.18502/kss.v3i10.3115.

[20] F. Haris, "IT Infrastructure Maturity Model (ITI-MM) A Roadmap to Agile IT Infrastructure," p. 118, 2010.

[21] R. Umar, I. Riadi, and E. Handoyo, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)," vol. 6, no. 2, pp. 193–202, 2019.

[22] J. David Patón-Romero, M. T. Baldassarre, M. Rodríguez, and M. Piattini, "Maturity model based on CMMI for governance and management of Green IT," *IET Softw.*, vol. 13, no. 6, pp. 555–563, 2019, doi: 10.1049/iet-sen.2018.5351.

[23] M. R. Ayyagari and I. Atoum, "CMMI-DEV Implementation Simplified," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, 2019, doi: 10.14569/ijacsa.2019.0100455.

[24] A. Chaudhary, S. Kolhe, and R. Kamal, "An improved random forest classifier for multi-class classification," *Inf. Process. Agric.*, vol. 3, no. 4, pp. 215–222, 2016, doi: 10.1016/j.inpa.2016.08.002.

[25] B. Rassa, "Capability Maturity Model Integration, Continued," *IEEE Instrum. Meas. Mag.*, vol. 6, no. 3, pp. 8–10, 2003, doi: 10.13140/RG.2.2.35219.94247.

[26] IBM, "An architectural blueprint for autonomic computing," *IBM White Pap.*, vol. 36, no. June, p. 34, 2006, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:An+architectural+blueprint+for+autonomic+computing+.#0%5Cnhttp://users.encs.concordia.ca/~ac/ac-resources/AC_Blueprint_White_Paper_4th.pdf

[27] I. Technology and A. Romanovs, "ITIL Self-assessment Approach for Small and Medium Digital Agencies," no. December 2014, 2015, doi: 10.1515/itms-2014-0021.

[28] "An Overview of the ITIL ® Maturity Model," no. September, 2021.

[29] M. Ranjani, "Green Computing - Maturity Model for Virtualization," *Int. J. Data Min. Tech. Appl.*, vol. 1, no. 2, pp. 29–35, 2012, doi: 10.20894/ijdmta.102.001.002.002.

[30] P. Kurp, "Green Computing," *Commun. ACM*, vol. 51, no. 10, pp. 11–13, 2008, doi: 10.1145/1400181.1400186.

[31] R. Sheikhpour and N. Modiri, "An approach to map COBIT processes to ISO/IEC 27001 information security management controls," *Int. J. Secur. its Appl.*, vol. 6, no. 2, pp. 13–28, 2012.

[32] G. F. Nama, K. S. Amin, and W. E. Sulistiono, "Assessment of Information Technology Governance Implementation Based on COBIT Framework 5 Focus on APO 04 Subdomain (Align , Plan and Organise)," vol. 20, no. 9, pp. 893–899, 2022, doi: 10.14704/nq.2022.20.9.NQ440099.

[33] M. Nyonawan, Suharjito, and D. N. Utama, "Evaluation of Information Technology Governance in STMIK Mikroskil Using COBIT 5 Framework," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 137–142, 2018, doi: 10.1109/ICIMTech.2018.8528138.

[34] P. Hidas, "Roadmap for Your Infrastructure — The Gartner Infrastructure Maturity Model," 2006.

[35] M.-H. Chuah and K.-L. Wong, "A review of business intelligence and its maturity models," *African J. Bus. Manag.*, vol. 5, no. 9, pp. 3424–3428, 2011, doi: 10.5897/AJBM10.1564.

[36] C. N. Pedrini and G. F. Frederico, "Information Technology Maturity Evaluation in a Large Brazilian Cosmetics Industry," *Int. J. Bus. Adm.*, vol. 9, no. 4, p. 15, 2018, doi: 10.5430/ijba.v9n4p15.

[37] J. V. Carvalho, Á. Rocha, and A. Abreu, "Maturity Models of Healthcare Information Systems and Technologies: a Literature Review," *J. Med. Syst.*, vol. 40, no. 6, 2016, doi: 10.1007/s10916-016-0486-5.

[38] J. Gomes and M. Romão, "Information System Maturity Models in Healthcare Information System Maturity Models in Healthcare," no. October, pp. 0–14, 2018, doi: 10.1007/s10916-018-1097-0.

[39] J. Gomes and M. Romão, "Information System Maturity Models in Healthcare," *J. Med. Syst.*, vol. 42, no. 12, pp. 0–14, 2018, doi: 10.1007/s10916-018-1097-0.

[40] H. Zijlstra, "Exploring Digital Suriname: The current state of digitalisation and the challenges that lie ahead," 2022, [Online]. Available: http://essay.utwente.nl/93340/%0Ahttp://essay.utwente.nl/93340/1/Zijlstra_MA_BMS.pdf