ISSN: 1978-0524

Information security analysis on physical security in university x using maturity model

Khaiurnnisak Nur Isnaini [a,1,*], Siti Alvi Solikhatin [a,2]

[a] University Universitas AMIKOM Purwokerto, Jl.Let.Jend.Pol.Soemarto, Purwokerto and 53127, Indonesia
[1] *nisak@amikompurwokerto.ac.id*[*]*; [2]sitialvi@amikompurwokerto.ac.id*
** corresponding author*

ABSTRACT

The threat of physical security can be from human factors, natural disasters, and information technology itself. Therefore, to prevent threats, we need the right tools to control current activities, evaluate potential impacts, and make appropriate plans so that business processes at X University will not be affected. This research starts by analyzing the problems that arise, followed by collecting the data needed, discussing the results, and making conclusions and recommendations that can be given. The method uses quantitative descriptive research. The research instrument uses interviews and questionnaire techniques. COBIT 5 is used as a framework for measuring the performance that is being implemented and will be achieved. Maturity models are used to measure current and future activities. The goal to be achieved is that the organization can create a physical security environment by the CIA principle (confidentiality, integrity, & availability). Positioning results are at level 3, meaning that the process is currently running in two main standard operating procedures. However, this evaluation specifically on the DSS5.5.5 subdomain (Providing Service Support-Managing physical security for IT Assets) in COBIT 5, and the results are still below the level 3 standard (Established Process), at 2.9 points. So, the right suggestion is to keep activities safe, one of which is to improve facilities and infrastructure, one of which is the use of biometric control in data center management rooms or other rooms with limited access.

Keywords:
Physical Security
COBIT 5
Maturity Model

I. Introduction

Information security is a direct process consists of physical security dominant and simple classification document[1]. The purpose of information security is to protect and preserve the value of an organization such as data and information[2]. The protection of information security can be done in several ways to ensure its integrity, confidentiality, and consistency. Also, to minimize the risk that can be happened anytime and endanger the process in the organization. The good reputation of an organization is judged by society from its commitment to integrity, confidentiality, and availability information[3]. A company's reputation is maintained certainly involves basic business needs, including the ability of the organization to maintain its function, ensure the operation runs smoothly by the needs of the information technology systems needed, maintain data collection and use, and safeguard its technological assets[1].

Threat [2] is an action or event that caused a disadvantage in terms of the fund, effort, good reputation, and bankruptcy. The threats that can interfere with a process business has happened from several factors, so the protection of information security is crucially needed. The form of threats consists of a hardware failure, software failure, human resource failure, nature failure, funding failure, external and internal failure.

Threat [4] is an action or event that caused a disadvantage in terms of fund, effort, good reputation and bankruptcy. The threats that can interfere with a process business has happened from several factors, so the protection of information security is crucially needed. The form of threats consists of a hardware failure, software failure, human resource failure, nature failure, funding failure, external and internal failure. Failure of human resources can be intentionally causing damage, illegal access, or leaking organizational data to third parties[5]. One of the solutions that can be taken if this happens is the use of traditional computing even though there is no full guarantee if it is safe, at least it can make the thief a little hassle when it will steal data or information that does not involve the system[6]

DOI: 10.26555/jifo.v14i2.a14434

A university must be able to ensure the safety and security of its organization because it is an important aspect of choosing an institution for its parents and students[7]. The threats mentioned above have also in some departments of University X, especially in physical security. According to [3] some things cause such threats to happened and can ruin the system such as unauthorized access, attack of hardware, wire management, displays, ergonomic side, networking, and human resources that use information technology. Now the fact is, there is no available room that specifically designed as a center of information technology, let alone customizes protection for it. According to [2] a central computer owned by University X should be controlled to prevent unauthorized usage. This activity can be done by adding a responsible task for each person to keep a central computer or information technology room safe. To make it worse, there is no standard procedure to handle unexpected damage such as an earthquake or wildfire. Another important physical threat found: there is no backup in the telecommunication network that causes such a disruption in accessing internet access. The impact is a failure of information processing in the system, e.g grade academic of students. Mentioned in [8] one of the alternatives that can be implemented is to provide a communication track via satellite, e.g using VSAT (Very Small Aperture Terminal) technology for the service provider. And also service providers can ensure that the fiber optic cable used is safe from all kinds of disturbances such as roadworks or government projects. so that the internet services provided can be maximized to university X.

Physical security threats can be in the form of access control systems, fire alarm systems, fire extinguishing systems, warning and evacuation management systems, engineering equipment monitoring and control systems, automatic systems and others—vasily. As stated by [9] that physical security strategies can be achieved through physical system components. The physical security component consists of prevention from conditional crime, system theory, and prevention from crime in the design environment. Physical security efforts can be done in various ways to create physical security scenarios that involve identification, analysis, and evaluation. Technical and organizational physical security is to measure prevention, cancellation, identification, warning, and feedback on the problem to support cybersecurity [10].

The security parameter in a system is highly important to the organization and is always aware of the threats and how to prevent it from damaging the assets. Security parameter consists of Physical Security, System Security, Application Security, dan Data Security. Physical security [11] is a term of security that focuses on the strategic ways of securing the user, staff or members of the organization, physical assets, and a working place from threats such as wildfire, unauthorized access, and natural disasters. The main goal of physical security is to protect information technology and prevent it from intentional or unintentional damage[8]. Physical security must be able to plan ways to protect all the assets of the organization, among others, in the form of ensuring that all personnel involved in the organization are safe and securing organizational assets in the event of a natural disaster[5]. Physical security is a security that covers the organization's building, available facilities, human resources, and other organizational assets so that it becomes important to be developed to achieve effective security in terms of resources, infrastructure, and systems[12]. Organizations can be innovative if they apply best practices for overall physical security[13].

Every organization has a parameter to measure the potential risk in terms of security. However, long-term use in the implementation of information technology can also pose potential threats that can cause risks during the implementation[14] . Security parameters in a system are very important for organizations which are always aware of threats and how to prevent them from damaging assets. The security parameters consist of Physical Security, System Security, Application Security, and Data Security. A physical security system is usually managed and operated by other security departments or organizations and some of them are created and supervised by the building owner[15]. University X now has implemented standard operating procedure but that hasn't reached all aspects of physical security that commonly be ignored its importance. It is known from the absence of the rules that restrict unauthorized people. Also, the staffs at University X are still unaware of the importance of physical security aspects. The aspects are company surroundings, premises, reception, server, workstation area, wireless access points, other equipment, access control, computer equipment, maintenance, wiretapping, remote access[8]. A standard operating procedure that has implemented is hardware usage in the internal campus, meanwhile, software management by certain departments hasn't been handled properly. The information security policy should cover all aspects. The goals are: to prevent illegal access to computer systems, to prevent data theft, to keep data integrity and to prevent damaging the information asset [16].

COBIT 5 is the best practice nowadays and is widely used as a measurement tool to design, to make and to evaluate activity related to information technology. COBIT is considered effective even though the mechanism is not easy because it has to go through various specific stages[17]. COBIT 5 provides complete package contents with areas that require further elaboration and renewal[18]. COBIT has the scope and objectives that can build objective controls for IT Auditors, help manage governance logically, and are a model of maturity for every process that runs[19]. COBIT which is used as an information technology management model implements internal controls and provides guidance for information technology resources including hardware, personnel, and others[20]. COBIT 5 can provide input in the form of recommendations from the information technology that is being applied and make improvements to management in the future[21]. According to [22] COBIT 5 is approvingly effective to manage rules, responsibility, and policy. COBIT 5 is functioned to assist the organization in measuring information technology to its utmost ability by keeping the advantage, risk management optimization, and using current resources. Maturity models are used to control information technology processes in an organization with the aim of determining current management positions and future management (expectations) [13]. Maturity model is a control tool so that the organization runs in accordance with the objectives. Information security maturity model is used to assess the scale of capabilities and maturity of an organization with the software used[23]. In addition, the maturity model is also used to find problems and determine the right way to solve them[24]. In summary, our paper's contributions are stated as follows:

1. We address the importance of security policy: in this case is limited to physical security, the personel security and the environment security to ensure that the resources are well managed and prevented from illegal access that may cause data destruction on both physical and digital
2. We offer that all organizations should be aware of physical security and have to establish the security policy as it is directly influenced their organization's sustainability
3. We also suggest that human resources need to get special briefing and have to be well-knowledged about the importance of physical security

In this domain there are ways to evaluate procedures that are more intensive than information security [25]. This research focused on one sole domain in COBIT 5: DSS5.5 (Decision Support System of Manage Physical Security to IT Assets). The domain explains the detail of physical security and elements related to it: authentification, access right, logical access, and user responsibility.

II. Method

A. Research Flow

The research flow is described below in Fig 1.

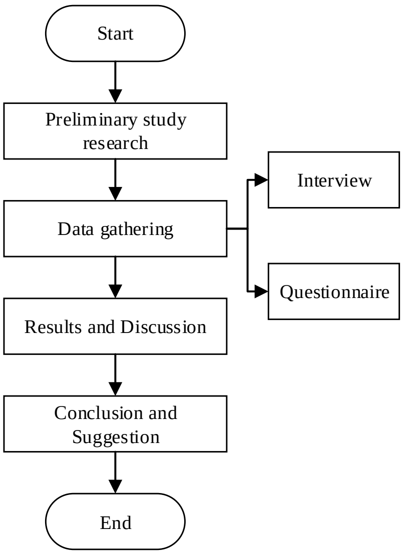


Fig. 1.Research Flow

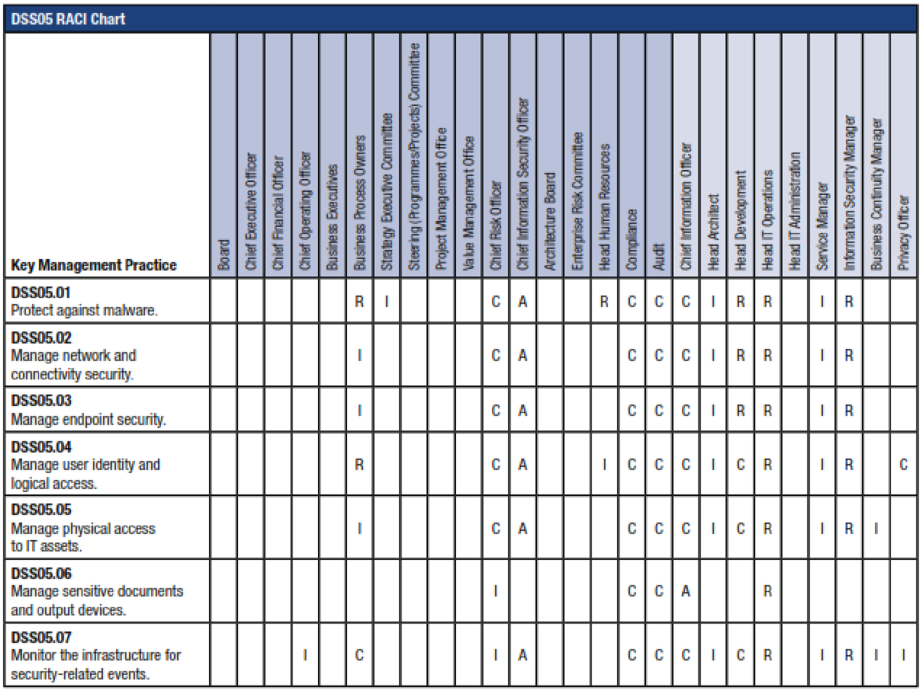
Description

1. Preliminary study research

   Preliminary study research begins with problem identification and potential errors that could happen and cause the new problem to appear in information security scope especially in the physical security of University X.

2. Data gathering

   Data gathering is conducted in two ways: an interview and a questionnaire. The interview is addressed to the IT staff and the head of Lembaga Penjaminan Mutu. The questionnaire is addressed to 83 active employees including IT staff and the head of Lembaga Penjaminan Mutu. The scale for this questionnaire is a Likert scale. Respondent dividing is based on the RACI table which functions is to understand responsibility level in the organization structure. RACI is used to map objectives that will produce appropriate recommendations [28]. Generally, this is how the RACI table describes it in Fig 2.



DSS05 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
DSS05.01 Protect against malware.						R	I				C	A			R	C	C	C	I	R	R		I	R		
DSS05.02 Manage network and connectivity security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.03 Manage endpoint security.						I					C	A				C	C	C	I	R	R		I	R		
DSS05.04 Manage user identity and logical access.						R					C	A			I	C	C	C	I	C	R		I	R		C
DSS05.05 Manage physical access to IT assets.						I					C	A				C	C	C	I	C	R		I	R	I	
DSS05.06 Manage sensitive documents and output devices.											I					C	C	A			R					
DSS05.07 Monitor the infrastructure for security-related events.				I		C					I	A				C	C	C	I	C	R		I	R	I	I

Fig. 2.RACI Chart

a. A chief information security officer is titled as Accountable for the head of IT staff and laboratory staff

b. Business process owner, head architect service manager, business continuity manager is titled as Informed for Bagian Kepegawaian Perencanaan dan Hukum, the head of IT staff and laboratory staff and Bagian Administrasi Akademik dan Pengajaran.

c. Head IT Operations dan Information Security Manager is titled as Responsible for The head of Lembaga Penjaminan Mutu dan Kepala IT dan laboratory staff.

d. Chief risk officer, compliance, audit, chief information officer, head development is titled as Consulted for all respondents who fill the questionnaire.

3. Result and discussion

   Discussion is about data analysis begins from statistic analysis of reliability and questionnaire validity, current analysis and future condition analysis, and gap analysis.

4. Conclusion and suggestion

   A summary is done based on the results from the previous part and then the suggestions which is relevant to the results are listed below.

B. Research Method

The research method used in this paper is descriptive quantitative. Quantitative research is research related to the quantification and analysis of variables to get results that involve numerical data analysis using statistical techniques[26]. Descriptive research is a research method that describes a situation that is happening according to the possibilities that exist systematically and the research instruments can be in the form of tests, questionnaires, interviews or observations[27].

III. Results and Discussion

A. General Description

Information technology used in University X is managed by two departments: Information Technology and Technical Computer Laboratory, and is being monitored by Lembaga Penjaminan Mutu. Lembaga Penjaminan Mutu in University X is functioned to maintain the quality of the two departments. If incidents happen the company has the right to evaluate and give suggestions according to applied standards. The details of the total number of employees are being described in Table 1.

Table 1. Total Number of Employees in 3 Departments

Department	Total Employees
Unit Pelaksana Teknis Teknologi Informasi	2 persons
Unit Pelaksana Teknis Laboratorium Komputer	11 persons
Lembaga Penjaminan Mutu	4 persons

The current policy is made related to physical security and is being monitored by Lembaga Penjaminan Mutu. The policy is described in several standard operational procedures, details in Table 2.

Table 2. Standard Operational Procedures in Using Information Technology

Department	Total Employees ***per unit**
Unit Pelaksana Teknis Teknologi Informasi	a) Quality procedures in registering an official email address for lecturers, staff, students, UKM and other departments. b) Quality procedures in integrating information systems. c) Quality procedures in network security, application and data d) Quality procedures in data storage institution.
Unit Pelaksana Teknis Laboratorium Komputer	a) Network installation procedure. b) Quality procedures in computer practice. c) Quality procedures of instruction to MikroTik registration.

Based on Tabel 2. above, it is concluded that the standard policy hasn't covered all aspects of security: preliminary plan, implementation, and evaluation especially on things related to physical security.

According to Indrajit (2014) the current condition in University X is mapped in 3 parts:

Security policy

1. Information security policy covers physical security that is not documented yet in each standard operational procedure specifically.
2. Personel security

   A specific rule from the related party about non-disclosure agreement hasn't been arranged yet for all employees who use the information technology (system and network). The rules are aimed to minimize the risk of user errors, theft, and facility misused.

3. Environment and physical security

   The system and network department at University X haven't built a computer central area that is separated from other users, this is to restrict unauthorized users from accessing it. Besides, system and network users haven't fully aware yet about the importance of a *clear desk* and *clear screen* which is crucial for illegal access prevention and data destruction on both physical and digital.

B. *Statistic and Analysis*

This research used statistic data analysis to understand the accuracy of results: validity test and reliability test. The tool that is being used is a questionnaire and actual maturity level about physical security.

The validity test in this research is implemented on the *bivariate person* method. The result of this test is retrieved and stated that all questions are valid. The questionnaire result is approved because the coefficient value (*r*-value) is larger than the *r* table. The *r* table is 0.213 with total questions = 7 and α = 0.05. For more details, see Table 3.

Table 3. Quetionnare Validity Test

Question	r-value
P1	0.770
P2	0.764
P3	0.739
P4	0.708
P5	0.747
P6	0.809
P7	0.765

The questionnaire reliability is being tested with the Cronbach-alpha test. The result of the Cronbach-alpha test can be seen in Table 4.

Table 4. Cronbach-alpha tes result

Case Processing Summary				Reliability Statistics	
		N	*%*	*Cronbach Alpha*	*N of Item*
Cases	Valid	82	98.8	.787	8
	Exclude [a]	1	1.2		
	Total	83	100.0		

[a] Listwise deletion based on all variables in the procedure

C. *Current condition analysis*

Capability level of current condition analysis is shown in Table 5.

Table 5. Capability Level

Capability Level	Description
Level 0 (Incomplete Process)	Process is not carried out
Level 1 (Performed Process)	The process is carried out and reached out the goal
Level 2 (Managed Process)	The current implemented process is managed according to the needs and the right work product that is being well handled and maintained.
Level 3 (Established Process)	The current implemented process has achieved the expected results according to set procedure
Level 4 (Predictable Process)	The current implemented process is running according to a set limit to reach the expected results
Level 5 (Optimizing Process)	The process is predicted to continue improving to fulfill the business's goal: current goal and future goal relevantly

The current condition in University X is described in the scheme of actual maturity level value in physical security, details in Fig. 3

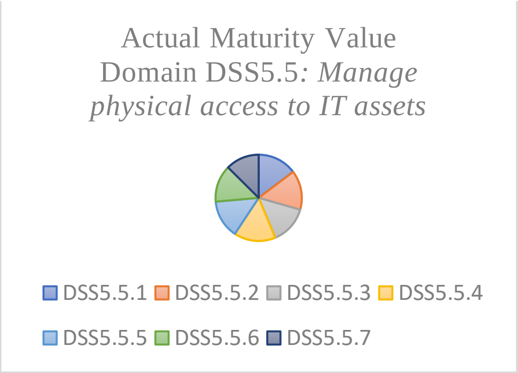


Fig. 3. Actual maturity level value

Description of domain sub item DSS5.5, details in Table 6.

Table 6. Actual maturity level value of domain sub item dss5.5

Items	**Score**
Managing demand and giving access to the computer facility	3.4
Making sure the access profile is conformed with job description and responsibility	3.4
Monitoring all modes of log leading to information technology sites	3.3
Instructing all personnel to display the visible identification anytime	3.6
The rule of a visitor to be monitored anytime in the location	3.3
The restriction of access to sensitive information technology system sites	3.2
Training of awareness for physical security periodically	2.9
Average	3.36

According to Table 6, the capability level that is reached in University X is 3.36. The level is in Level 3: Established Process. This level shows that the process already run and conform according to set procedure. The process has identified the responsibility of each department that manages the physical security, though not entirely conducted.

The implementation does not yet cover all aspects of information security especially in terms of awareness from users that already been described in Table 6. In the table, we can see that user awareness about physical security is not in accordance with expectation and is below the average point of the measured subdomain. That can happen because the standard rules are not arranged yet, with no planning and evaluation of threats natural disasters that can happen and endanger physical security at University X.

D. *Gap Analysis*

Gap analysis of actual maturity value with the expectation value of the current process in University X especially in terms of information security login access and user identity is retrieved from the gap between expectation capability level and current capability level. The graphic value of the gap in using the information technology in University X is described in Fig. 4.

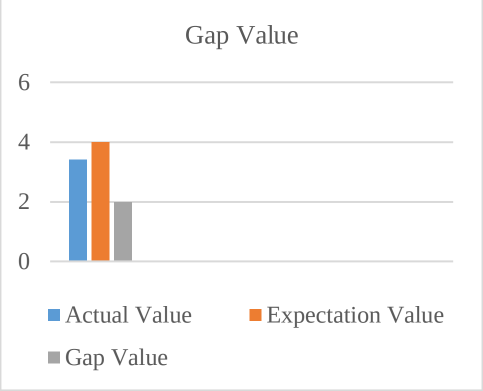


Fig. 4. Gap analysis

Result of gap analysis is given in detail in Table 7.

Table 7. Gap Value

Items	Score
Managing demand and giving access to the computer facility	3.4

According to Table 7, the gap value is 0.64. Specifically, the result shows that the largest gap is in user awareness about physical security. The gap arises because the current standard operational is only focus on the usage of hardware, software, account, and awareness about threats to physical security at University X.

IV. Conclusion and Suggestions

The analysis and measurement of maturity level show the result of University X is in Level 3, Established Process. At this level, University X is rated to already conform to the standard operating procedure on its activities led by the Department of Information Technology and Computer Laboratory to reach the expected goal. But in certain conditions, weakness is found related to user awareness about physical security. And it's confirmed by the result of the maturity level in 2,9. Besides, the Disaster Recovery Plan isn't arranged yet in the Standard Operational Procedure framework and caused the handling process of incidents and risk management is difficult to conduct properly. Information security management in the physical security field has to improve its employee's capability in order to reduce the gap. This part is important so that the policy that has been arranged can be obeyed by all elements of University X optimally. And from that point on, suggestions are needed to reach the goal: 1) Human resources as information technology users get special training about information security specifically in physical security according to the set procedure designed by Lembaga Penjaminan Mutu; 2) The infrastructure and facilities can be added: fingerprint or specific biometric control in the data center and information technology management room; and 3) The policy or rule can be added: item of the standard operation of a current set procedure named *Disaster Recovery Plan*.

Acknowledgment

Big gratitude to Allah SWT for His mercy so the writers can finish this paper well. Special thanks to Mr. Didit Suhartono, M.Kom. and Siti Alvi Solikhatin, M.Kom. who helps me throughout the process of writing this research entitled as Information Security Analysis on Physical Security at University X.

References

[1] M. E. Whitman and H. J. Mattord, *Principles of Information Security Fourth Edition*. 2011.

[2] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "A process framework for information security management," *Int. J. Inf. Syst. Proj. Manag.*, vol. 4, no. 4, pp. 27–47, 2016.

[3] IBISA, *Keamanan Sistem Informasi*. Yogyakarta: CV ANDI OFFSET, 2011.

[4] IBISA, *Keamanan Sistem Informasi*. Yogyakarta: ANDI OFFSET, 2011.

[5] M. A. H. H. Shohaieb, "Effect Of Physical Security Initiatives On Supply Chain," vol. 2, no. 1, pp. 18–35, 2018.

[6] F. Abdi, C. Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems," *Proc. - 9th ACM/IEEE Int. Conf. Cyber-Physical Syst. ICCPS 2018*, pp. 10–21, 2018.

[7] A. M. Razmy and A. Jabeer, "Association between the Performance of the University Security Officers and Their Physical Fitness: A Case Study," *OALib*, vol. 4, no. 6, pp. 1–7, 2017.

[8] IBISA, *Physical Security*. Yogyakarta: CV ANDI OFFSET, 2013.

[9] M. P. Coole and D. J. Brooks, *Physical Security: Best Practices*. 2019.

[10] D. Antonucci, *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*. Belgium: John Wiley & Sons, Inc, 2017.

[11] M. E. Whitman and H. J. Mattord, *Principles of Information Security Fourth Edition*, 4th ed. Boston: Course Technology, 2011.

[12] S. Moses and D. C. Rowe, "Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques," *Int. J. Inf. Secur. Res.*, vol. 6, no. 2, pp. 667–676, 2016.

[13] I. U. A. A. I. L. A. M. K. Idierukevbe, "Physical Security Best Practices," *J. Phys. Secur.*, vol. 12, no. 3, pp. 15–29, 2019.

[14] A. F. Apriliana, R. Sarno, and Y. A. Effendi, "Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 54," *2018 Int. Conf. Inf. Commun. Technol. ICOIACT 2018*, vol. 2018–Janua, pp. 373–378, 2018.

[15] M. Lalonde, "Combining Strengths .," The Conference Board of Canada, Ottawa, Canada, 2018.

[16] P. R. E. Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*. Yogyakarta: Graha Ilmu, 2014.

[17] A. Arief and I. H. A. Wahab, "Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia)," in *Proceedings - 2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2016*, 2017, pp. 388–392.

[18] W. Al-Ahmad and B. Mohammed, "A code of practice for effective information security risk management using COBIT 5," *2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015*, pp. 145–151, 2016.

[19] M. Motii and A. Semma, "Towards a new approach to pooling COBIT 5 and ITIL V3 with ISO/IEC 27002 for better use of ITG in the Moroccan parliament," *Int. J. Comput. Sci. Issues*, vol. 14, no. 3, pp. 49–58, 2017.

[20] W. Gunawan, E. P. Kalensun, A. N. Fajar, and Sfenrianto, "Applying COBIT 5 in Higher Education," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, 2018.

[21] A. Tantiono and N. Legowo, "Information System Governance in Higher Education Foundation using COBIT 5 Framework," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2798–2811, 2020.

[22] M. Wolden, R. Valverde, and M. Talla, "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system," *IFAC-PapersOnLine*, vol. 28, no. 3, pp. 1846–1852, 2015.

[23] [R. Umar, A. Fadlil, and A. I. Putra, “Analisis Forensics Untuk Mendeteksi Pemalsuan Video,” *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 2, p. 193, 2019.

[24] R. R, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *Int. J. Comput. Appl.*, vol. 141, no. 8, pp. 1–6, 2016.

[25] I. Riadi, I. T. R. Yanto, and E. Handoyo, "Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 821, no. 1, 2020.

[26] O. D. Apuke, "Quantitative Research Methods : A Synopsis Approach," *Kuwait Chapter Arab. J. Bus. Manag. Rev.*, vol. 6, no. 11, pp. 40–47, 2017.

[27] H. Atmowardoyo, "Research Methods in TEFL Studies: Descriptive Research, Case Study, Error Analysis, and R & D," *J. Lang. Teach. Res.*, vol. 9, no. 1, p. 197, 2018.

[28] I. A. R. I. R. Prihandi, "COBIT 5 for Improving Production Performance using DSS Domain," *Int. J. Innov. Technol. Explor. Eng.*, vol. 9, no. 4, pp. 678–681, 2020.

D. M. Selvianti *et al.*, “Perancangan service catalogue management dan service level management pada layanan it pusair Puslitbang Sumber Daya Air , Bandung,” *J. Sist. Inf.*, vol. 5, no. 4, pp. 436–445, 2015.