Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 21, No. 2, Maret 2022, pp. 317∼326
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v21i2.1311

Evaluation of Basic Principles of Information Security at University Using COBIT 5

Khairunnisak Nur Isnaini[1], **Didit Suhartono**[2]
[1,2]Universitas Amikom Purwokerto, Indonesia

Article Info

Article history:

Received June 26, 2021
Revised September 01, 2022
Acceptedmm March 15, 2022

Keywords:

Information Security
COBIT 5
Evaluation

ABSTRACT

Information security issues commonly arise in a company and institution, including those in University. Some of the threats and attacks are unauthorized access, system user accountability, and logical and physical issues. This study reveals the obedience rate of the information security principle in Universitas Amikom Purwokerto and provides a recovery strategy. The domains being used were APO13, DSS5, and MEA3. The researcher employed a descriptive quantitative method by having documentation, interview, and administering a questionnaire to the respondents. The respondents were 83 employees who got selected by using the purposive sampling technique. The result shows that the capability level is in level 3, known as the established process. It means that the employees have applied the current procedure, even though they have not applied information security management. The proposed refinement strategy emphasizes the security policy, classification and asset management, physics and environment security, and business continuity management. The gap can be fixed by implementing the proposed refinement strategy. Future researchers may evaluate obedience based on the identified variables by keeping the standard in mind.

Corresponding Author:

Khairunnisak Nur Isnaini,
Department of Informatic,
Universitas Amikom Purwokerto, Indonesia
Email: nisak@amikompurwokerto.ac.id

1. INTRODUCTION

Information is one of the most valuable assets for an organization because it is a strategic resource to increase the business value [1]. Any information could be collected, managed, and disseminated in documents, printed and electronic. While doing that information, we should pay attention to its security, including its confidentiality, integrity, and availability. These aspects have a prominent role in increasing excellence, image, and organizations that have important assets.

Informatio n security protection aims to prevent losses for the sustainability of the agency or organization activities carried out by all participating parties. The organization is expected to have control over many policies and procedures to ensure these objectives. Several technical steps should be applied supported by the right management policies and procedures [1][2]. Universitas Amikom Purwokerto should also carry out its implementations.

Universitas Amikom Purwokerto is a private university that applies various information technologies to support daily activities. However, it is still in the air whether the security has protected the use of information technology. According to the ten elements of information security, that university can get the problem of security threats. It is caused by several events, like a misuse of an internet user account to an unauthorized access system. In addition, from the aspect of asset classification and control, the responsibilities of the that university are still unclear. A smart system that the administrator from the study program uses can also be accessed by the administrator of academic administration for the same rights. As a result, information leakage possibly happens if there is no control for its usage.

Moreover, in communication and operation management, security gaps have arisen because there is no Disaster Recovery Plan to deal with the predicted trouble. Server down is one of the mostly-faced trouble when the students fill study plans in their accounts. In the aspect of physical and environmental security, no longer-used important documents in the form of hard copy that are no longer used are not automatically destroyed. It makes the document could be easily found by others and potentially used by the abuser. In contrast, according to [3], The computer administrator should control access allowance to the site. Referring to the 10 elements of information security [1] Amikom University Purwokerto ideally should be able to implement all the existing elements so that business processes run well. However, some of them are not suitable. It causes problems to be encountered, including the possibility of unauthorized access or information security gaps that can arise due to the lack of an appropriate information security management.

Universitas Amikom Purwokerto currently made policies for the operation, including the procedure of information system deletion, institutional data storage, and Mikrotik login registration. These procedures contain information security aspects that have been obeyed by employees, one of them is to keep account confidentiality. Nevertheless, the procedures have not been able to protect the information. No steps are explaining the procedure to secure the data. None also the steps explaining the solution that could be taken when the employees or the third parties do a violation. This case is still in planning. 'Planning' means that the policies are still in consideration and examination to apply the standard of ISO 27001:2013 or ISO 27002 using the modeling standard from SANS.org. Information leakage came as the result of minimum alertness.

According to [4], security is important in information systems, especially in protecting confidential matters; and storing and managing existing information assets. The application of a security system is aimed to overcome the technical and non-technical problems and obstacles that can affect the system performance [5]. Information security is a must to keep the system from being threatened [6]. According to Farida and Rahajeng in [7], security is important since it deals with information accuracy. If the unexpected user could access the information, it could be untrustworthy because of some possible changes. Higher education is one of the institutions that provide services to the community. Any information should be given to the students, employees, and other parties if needed [7]. In giving this service, the utilization of information technology is increase. It could give better efficiency and effectiveness [8]. Security issues affect the control mechanism in protecting the computer networks from abusers. This is because the ease of information access could make it less accurate due to possible changes [6].

COBIT belongs to the information technology control framework for enterprises [9]. In COBIT 5, some domains are used to standardize measurement, like Evaluate, Direct, and Monitor (EDM), Align, Plan, and Organise (APO), Build, Acquire, and, implement (BAI), Deliver, Service, and Support (DSS), Monitor, Evaluate, and Assess (MEA). COBIT 5 [10] can evaluate the state of the information technology and give a solution as the result of evaluation dealing with compliance capability on the basic principles of information security.

Several researchers with various specific objectives have carried out research using COBIT. In research [7], COBIT analyzes information security with CMMI (Capability Maturity Model Index) method. The purposive sampling technique is involved in selecting the respondents. Another research was conducted by [11]. COBIT 5 is applied to audit the information system security using the APO13 (Manage Security) to protect it from security issues. Research [12] uses COBIT 5 to create an operational procedure collaborating with ITIL V3 to measure the Problem Management of information technology using DSS5.3 (Manage Problems). COBIT 5 is also used by [13] as the standard to measure information security governance using the DSS5 (Manage Security Service) domain. COBIT 5 is used by [14] to compare three aspects of information security using the DSS5 (Manage Security Services)

domain and NIST SP 800-55 framework. COBIT 5 has also been used by [15] to evaluate information security governance in collaboration with APO13 dan DSS5 domains. COBIT 5 is also used to analyze the results of the ”smart prodi” system performance using the Delone Mclean approach [16]. Other researchers use COBIT 5 to measure the governance of a company with a calculation model referring to ISO/IEC 15504 [17].

This recent study chooses APO13, DSS5, and MEA3 as the appropriate domains to measure the information security compliance of the research object. APO13 dan DSS5 contains information security management guidelines to analyze the existing security services. MEA3 contains guidelines that are used to evaluate the result of the test. The use of the MEA3 domain is also expected to follow up the previous studies about APO13 dan DSS5 domains.

This research refines the previous research by integrating the APO13, DSS5, and MEA3 domains. This can be make the evaluation results, namely the improvement strategy provided will be an appropriate solution to overcome the problems that arise. APO13 provides an overview as a reference domain in making an information security policy or procedure. DSS5 provides an overview as a reference domain for the implementation of information security services in both physical and digital forms. Meanwhile, MEA3 provides an overview as a reference domain for making evaluation results in accordance with problems that arise, monitoring, and assessing compliance with what has been made, used, and carried out, especially within the Amikom University Purwokerto. In addition, the improvement strategy provided will refer to 3 principles of information security which are translated into 10 aspects according to Indrajit with the aim of obtaining specific and targeted results.

Evaluation is carried out to solve the problems due to information security risks, like cost overruns, suboptimal use of assets, and improper maintenance of infrastructure [18]. Seeing the results of previous studies , the previous studies has proven that information security is still worthy of being the topic of analysis, especially in the awareness attitude towards data security. The purpose of this study is to obtain the correct measurement results in terms of information security. It is expected that the upcoming strategies can be taken into consideration in policymaking. The policies aim to strengthen information security and minimize the risks that possibly arise in the future due to information security threats and business attacks.

2. RESEARCH METHOD

2.1. Method of Data Collection

The method of data collection are documentation studies, interview, and questionnaire. Documentation studies are conducted to have an understanding of documents containing the information of procedure, policies, and rules in the information security of Universitas Amikom Purwokerto. Unstructured interviews are conducted by doing the direct questions and answers with the interviewees. They are the Head of UPT Pengembangan Laboratorium dan Teknologi (PLT) and the Head of Lembaga Penjaminan Mutu (LPM). Questionnaires are distributed with the consideration of the purposive sampling technique. This technique has been used in research [19] because not all populations are suited to the criterion. The participant should be employees and users of information technology. The question is given to participants correspond to their roles and responsibilities. Meanwhile, RACI Chart is used to select the participants of the questionnaire. RACI Chart [20] shows the distinctive roles among the participants related to its Responsibility, Accountability, Consultation, dan Information to the main activities. In addition, RACI Chart is also used to give a picture of the process of Assessment Maturity Level so that the interview is right on the target. Responsible, Accountable, Consulted, and Informed are the four aspects used to select the corresponding and competent respondents. The collected data is presented in table 1, entitle Key Management Practice.

Table 1. Key Management Practice

Variable	RACI Chart			
	Responsible	Accountable	Consulted	Informed
Chief Executive Officer	2	-	2	1
Head IT Operation	9	-	3	1
Business Process Owners	3	-	1	-
Compliance	2	1	11	-

Based on table 1, Key Management Practice has the highest score at the responsible and consulted levels compared to the other levels. The respondents are the Chief Executive Officer, that is General Chair; the Head of IT Operations, that is the Head of UPT PLT; Business Process Owners, the Head of LPPM. And the Compliance, that is a general employee.

2.2. Method of data Analysis

A statistical test is done using a measurement scale. There is also a test of validity and data reliability. The Likert scale is used to measure the interval data. This scale has a range value from positive to negative by giving a score from 1 to 5. The Likert scale has been used by the previous researcher [21] to make a questionnaire for analyzing the level of distribution assets management using COBIT 5 and other frameworks. A validity test is done to check the application of the statistical test in measuring the overall data. The validity test is done by seeing the correlation of Bivariate Pearson (Product Moment Pearson). A question could be categorized as valid if the correlation of its coefficient (r) is counted to geq the correlation coefficient (r). The correlation coefficient (r) constant table is examined using a two-tailed test method with a level of significance $(\alpha = 0.05)$. A reliability test is done by giving a questionnaire to see its consistency. Consistency means that it could be used several times. The test uses Cronbach's Alpha. It could be said as reliable if it has a good reputation with the scores 0.7 and 0.8.

2.3. Gap Analysis

In this research, gap analysis is conducted to find out the distance between the interview results, in this case are the actual value and the value of expectations (value of expectations that have been determined). Gap analysis also becomes the reference tool to make recommendations. The recommendations are emphasized on control objectives that have the highest gap values. Thus, the recommendations can be a solution to the problems that arise.

2.4. Research flow

The flow of the research is presented in figure 1. The research is divided into four steps. This research is started with the identification of problems. Then, the scope of research is decided. Data collection is conducted by reading the documents, doing interviews, and distributing the questionnaire. The interviewees are IT staff and employees who work with data security. The last step in data collection is distributing a questionnaire based on the domain of the employee. Data analysis begins with arranging the result of the actual value of employee compliance level. Analysis of the interview result is also conducted to estimate the expected value of compliance level. The last step on data analysis is doing gap analysis dealing with the actual value and the expected value of compliance level. The last overall step in this research is started by giving the improvement strategy plan based on the result of the analysis. The conclusion and suggestion are also delivered to the next research.

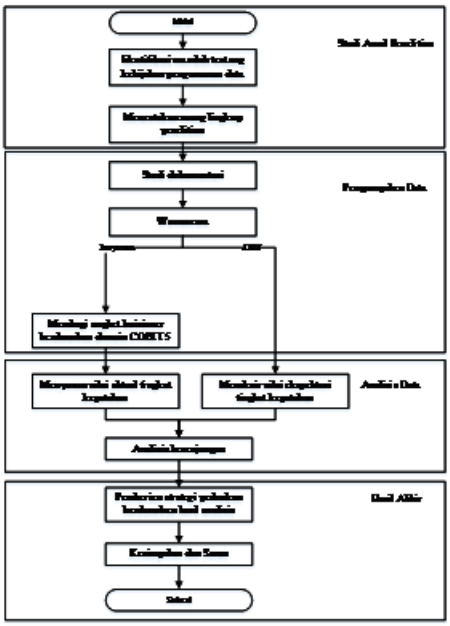

Figure 1. Research Flow

3. RESULT AND ANALYSIS

3.1. Analysis of Current Condition

Information technology is currently regulated and managed by UPT (PLT) and is supervised by (LPPM) or LPM (Lembaga Penjaminan Mutu) to maintain its quality. There is a regulation about the implementation procedure of information technology usage. The procedure can be seen on table 2.

Table 2. Key Management Practice

No	Quality Procedure
1	The quality procedure of email registration for students, lecturers, employees, students' activity unit, and work unit.
2	The quality procedure of information system integration.
3	The quality procedure of data security, application, and data complaint.
4	The quality procedure of institutional data storage.
5	The procedure of network installation.
6	Procedure for the implementation of computer laboratory practicum.
7	Procedure for the work instruction of MikroTik login registration.

Based on the operational procedure presented in table 2, it could be said that there is no policy for the procedure of data security. According to [1], the findings is mapped into ten aspects of information security such as in Security Policyaspect, the policy that is stated on operational procedure has not declared about the data security organization. In security organization, employees awareness of data security on using information technology has not been evaluated yet. In assets qualification and control, the ownership of assets related to the information technology used cannot be determined specifically. In personal security, Universitas Amikom Purwokerto does not have a special scheme to monitor the new or existing employees to prevent the risk of information leakage. In the other side on physical and environmental security, the university does not have a special room as the computer center that can only be accessed by certain parties. The workspace of the information technology division still unites with other divisions so that unauthorized access possibly happens. Also in communication and operation management, Disaster Recovery Plan has not been arranged by the university. In access controls aspect, the control of access is still minimum and unprotected from computer network hacking. In system development and maintenance, the required information security has not been completed. Negligence by the employees in maintaining information confidentiality, information availability, and data agency integrity possibly happens. For business continuity managements aspect, there are no implementation and development of business continuity to prevent and reduce the potential risks. And for the suitability, the existing operational procedure does not contain legal aspects that can be implemented to the violation done by the employees dealing with information security. The legal aspect can be arranged to regulate criminal law, civil law, legislation, and obligation as agreed.

3.2. Data Analysis

The data analysis is divided into several steps such as validity test, reliability test, and analysis of capabilities Level based on the result of the questionnaire. The questionnaire is distributed to 83 respondents based on the RACI chart in COBIT 5 domains, which are APO13, DSS5, dan MEA3. In validity test, The distributed questionnaire consists of 86 statements coming from three domains. If the r count for each statement is greater than r in the table and the value of r is positive, then the statement is valid. Based on the analysis, the statements used to measure employee's Compliance with data security policies have coefficiency greater than r on the table. R on the table is 0,2159 with n = 83 and = 0,05. It can be concluded that the statements are valid. In reliability test, results coming from the reliability test are presented in table 3 and table 4.

Table 3. Result of case processing summary

Case processing summary		
	N	%
Case Valid	83	100
Excludeda	0	0
Total	83	100

Table 3 shows that the output case processing summary of 83 respondents was all well observed. It is illustrated in the Excluded value which is declared to be 0. The output case processing summary also explains that there are no missing samples. Based on the results in table 3, the data can be executed with statistical calculations according to the needs of the researcher.

Table 4. Result of Reliability Test

Reliability Statistics	
Cronbach's Alpha	N of item
0,989	86

Table 4 shows that Cronbach's Alpha value is 0,989, which is good and reliable. This reliability test tested 86 question items contained in the questionnaire. Based on the theory proposed by [22], Cronbach's alpha value of more than 0,6 is good. It means that the statement items from the questionnaire results are very good and reliable

In analysis of capabilities level, questionnaire results presented information od the actual value for each domain. Here are the descriptions of APO13s domain. The domain contain an overview as a reference domain in making an information security policy or procedure. The actual value of capabilities level in the APO13 domain can be seen in table 5.

Table 5. Actual value of capability level in APO 13 domain

Statements APO13 (Manage Security)	Value
APO13.01 Establish and maintain an ISMS	3,47
APO13.02 Define and manage an information security risk treatment plan	3,39
APO13.03 Monitor and review the ISMS	3,32
Average of Capability Level	3,39

Based on table 5, the actual value of capability is 3,39. The value is positioned at level 3, that is, Established Process. At this level, Universitas Amikom Purwokerto has made the operational procedure for information technology organization. Yet, the standard of operations is under the Information Security Management System. Management of information security risk plan, the procedure of data security, and the Control of Information Security Management System have not been established. This condition causes the university to have no policies for the steps of securing data. The use of information technology depends on usage procedures without any specific limitation to protect their assets.

The second domain is DSS5. The domain DSS5 contain an overview as a reference domain for the implementation of information security services in both physical and digital forms. The result of the actual value from the level of capability in the DSS5 domain is presented in table 6.

Table 6. Actual value of capability level in DSS 5 domain

Statements DSS5 (Manage Security Services)	Value
DSS05.01 Protect against malware	3,39
DSS05.02 Manage network and connectivity security	3,46
DSS05.03 Manage endpoint security	3,38
DSS05.04 Manage user identity and logical access	3,58
DSS05.05 Manage physical access to IT assets	3,56
DSS05.06 Manage sensitive documents and output devices	3,35
DSS05.07 Monitor the infrastructure for security-related events	3,25
Average of Capability Level	3,39

Based on the information presented in table 6, the actual value of capability level 3,39. It can be categorized into level 3, that is, Established Process. Universitas Amikom Purwokerto has made an operational standard in this level, as seen in table 2 but still not specifically related to data security policies and their control of the process. They saw the management if physical access to information technology assets, the computer center room should be separated in one room. The management of sensitive document

and output devices is still neglected. They have no awareness to clear desk dan clear screen on each room to protect the document from the unexpected parties. The operational procedure does not contain the specific regulation to protect the systems from malware and secure the network and connectivity. There is no punishment for the potential violations.

The third domain is MEA3. The domain MEA3 contain an overview as a reference domain for making evaluation results in accordance with problems that arise, monitoring, and assessing compliance with what has been made, used, and carried out, especially within to the university. The test result of capability level using the MEA3 domain is presented in table 7.

Table 7. Actual value of capability level in MEA domain

Statements MEA3 (Monitor, Evaluate and Assess Compliance with External Requirements)	Value
MEA03.01 Identify external compliance requirement	3,35
MEA03.02 Optimize response to external requirements	3,4
MEA03.03 Confirm External Compliance	3,38
MEA03.04 Obtain assurance of external Compliance	3,32
Average of Capability Level	3,36

Based on table 7, the actual value of capability level is positioned at 3,36. It belongs to level 3, which is the Established Process. At this level, Universitas Amikom Purwokerto has made an operational procedure for information system deletion, institutional data storage, and MikroTik login registration. Nevertheless, the procedure does not state how to protect information technology assets like the Disaster Recovery Plan or Business Continuity Plan as recovery steps. The result of measurement toward Capability Level of employee compliance in securing each domain's data is seen in table 8.

Table 8. Capability Level

Domain	**Value**
APO 13	3,39
DSS 5	3,39
MEA 3	3,36
Average Capability Level	3,38

The result of measurement for capability level is 3,38, and it belongs to level 3, namely Established Process. In general, Universitas Amikom Purwokerto has made an operational standard in this level but procedure does not state how to protect information technology assets.

3.3. Analysis of Expected Condition

In general, it can be concluded that university has a plan to make a policy using the standard of ISO 27001:2013 and ISO 27002. The existing operational procedure can be revised by adding some statements related to risk management. It is also expected that the procedure contains the regulation to improve the monitoring and evaluation considering the policy issued. The upcoming policies will include user policy, its policy, general policy, dan partner policy.

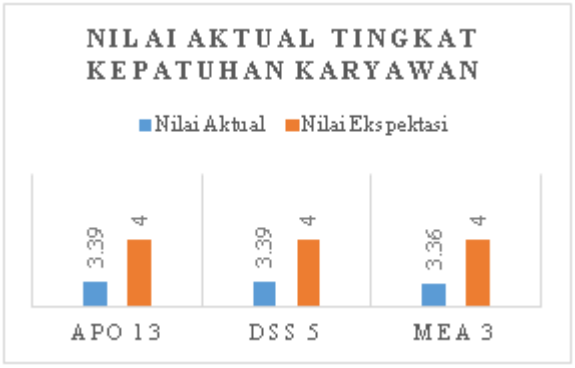

Figure 2. Current Value (as-is) of Employee Compliance Level

3.4. Gap Analysis

Gap analysis is obtained by the assessment evaluated before and after the measurement using COBIT 5 framework. In general, there are some possibilities such as some employees of Universitas Amikom Purwokerto comply with the basic principles of information security because they already know about it. The other side, some employees comply with the basic principle of informstion security because they already know and have run the operational procedure. But, some employees in the university do not comply with the basic principle of information security. And some employess do not comply with the basic principles of information security because they do not know about it, and X has not made any policy relates to information security. The gap value per subdomain is presented in table 9.

Table 9. Gap value per domain

Domain	Level of expected value	Level of actual value	Level of gap value
APO13.01	4	3,47	0,53
APO13.02	4	3,39	0,61
APO13.03	4	3,32	0,68
DSS05.01.	4	3,39	0,61
DSS05.02	4	3,46	0,54
DSS05.03	4	3,38	0,62
DSS05.04	4	3,58	0,42
DSS05.05	4	3,36	0,64
DSS05.06	4	3,35	0,65
DSS05.07	4	3,25	0,75
MEA03.01	4	3,35	0,65
MEA03.02	4	3,4	0,6
MEA03.03	4	3,38	0,62
MEA03.03	4	3,32	0,68
MEA03.04	4	3,47	0,53

Based on table 9, it can be concluded that the smallest gap value is on sub-domain DSS5.4 (Manage user identity and logical access), which is 0,42. It means management and control have run and almost close to the expected value. On the contrary, the greatest gap value is on sub-domain DSS5.7 (Monitor the infrastructure for security-related events), which is 0,75. It means that employee's Compliance and Awareness of X should be improved. The overall gap level is counted based on the average of every domain. The results are shown in Table 10.

Table 10. Overall gap level

Domain	Level of expected value	Level of actual value	Level of gap value
APO 13	4	3,47	0,53
DSS 5	4	3,39	0,61
MEA 3	4	3,32	0,68
	Average of gap level		0,62

As presented in table 9, the greatest gap value found in APO 13.03 is 0.67, DSS05.07 is 0.75, and MEA03.04 is 0.68. The gap occurs between information security policy, both from an internal and external factor. The policy of securing data do not cover the basic principle of information security, although some principle quality procedure has been defined. In general, the average gap value is 0,62, with the highest gap value is on MEA3. It contains information security policy related to its policy, rules, procedure, and regulation from several aspects. The findings of capability level findings are expected to help the employees as the information technology users understand the rules, procedures, and regulations for securing data to protect personal and institutional assets.

3.5. Refinement strategies

Some refinement strategies are proposed by several aspects such as the security policy, procedure making of information assets security is classified based on security, like user policy, policy, general policy, and partner policy. In security policy, PLT or the division makes a regular periodical schedule for controlling and monitoring information technology usage. In assets classification and control, UPT PLT evaluates and competes the quality procedure coordinated with other division that relates to control system. In personal security, UPT PLT compiles procedures for user responsibilities specifically. In physical and environmental security, UPT PLT proposes physical security, that is demanding a particular computer room. Also in communication and operation management, Universitas Amikom Purwokerto builds Disaster Recovery. In access control, UPT PLT designs a procedure containing the rules for user id, password management, access level, and responsibilities. And then in system development and maintenance, Universitas Amikom Purwokerto has proposed a team as controller, user, and tester to examine the controlling procedure. In business continuity management, the university must implements Business Continuity Planning, including a Disaster Recovery Plan. And in suitabilitys aspect, the university have to collaborates with legal institutions to obtain information and suggestion in compiling the regulations of information technology management and violation or abuse to the assets.

4. CONCLUSION

The study reveals the conditions based on the result of assessment before and after measurements. The overall domain shows that the capability level is 3.38, positioned at level 3, an established process. This research has several improvement strategies that refer to the information security aspect and are compiled based on the results of field findings and statistical analysis that not many researchers have discussed in detail the recommendations given. Refinement strategy is proposed based on the highest gap value to be implemented in information security aspects, such as security policy, assets control, classifications, physical and environmental security, and business continuity management. This research can be said to have not been maximized because the improvement strategies provided have not achieved technical results such as making blue prints or designs for each of the existing strategies that are related to the continuity of ongoing business processes. Further research can be done using NIST 800-34 Rev 1 or ISO 22301 related to Disaster Recovery Plan and Business Continuity Plan.

REFERENCES

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

[2] K. Marzuki and A. Apriani, "Evaluasi Penerapan Teknologi Informasi E-Learning Pada Kampus Swasta Menggunakan Cobit 4.1," *Jurnal Bumigora Information Technology (BITe)*, vol. 1, no. 2, pp. 161–166, 2019.

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

[4] P. P. G. Pertama and I. W. Ardiyasa, "Audit Keamanan Sistem Informasi Perpustakaan STMIK STIKOM Bali Menggunakan Kerangka Kerja COBIT," *Jurnal Sistem Dan Informatika*, vol. 13, no. 2, pp. 77–86, 2019.

[5] R. R, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *International Journal of Computer Applications*, vol. 141, no. 8, pp. 1–6, 2016.

[6] E. Kurniawan and I. Riadi, "Security Llevel Analysis of Academic Information Systems Based on Standard ISO 27002: 2013 Using SSE-CMM," *International Journal of Computer Science and Information Security (IJCSIS),*, vol. 16, no. 1, pp. 139–147, 2018.

[7] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *Jurnal Sistem Informasi Bisnis*, vol. 9, no. 1, pp. 47–54, 2019.

[8] H. Ghasali and K. Christianto, "System Information Audit with COBIT 4.1 and Balanced Scorecard Framework (Case Study: PT. Boga Dimsum Indonesia)," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 2, no. 2, pp. 560–565, 2018.

[9] L. Lelah and Toto Suharto, "Tata Kelola Keamanan Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus pada Dinas Komunikasi dan Informasi Kota Sukabumi)," *Jurnal Gaung Informatika*, vol. 12, no. 1, pp. 46–55, 2019.

[10] E. Surjandy; Fernando, A. Condrobimo, and M. R. Yudho, "Evaluasi Penerapan IT Governance pada Bank Berdasarkan Cobit 5 (Study Kasus Pada Bank XYZ) Evaluation Implementaion of IT Governance at Bank Xyz Based On Cobit 5 (Case Study at Bank XYZ)," *Jurnal Teknologi dan Ilmu Komputer (JTIIK)*, vol. 7, no. 3, pp. 453–460, 2020.

[11] I. J. Aritonang, E. D. Udayanti, and N. Iksan, "Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13)," *Information Technology Engineering Journals*, vol. 3, no. 2, pp. 3–7, 2018.

[12] F. Effendy and E. Hariyanti, "Manajemen Masalah Teknologi Informasi Berdasarkan Kerangka Kerja ITIL V3 dan COBIT 5," *Jurnal Sistem Informasi Bisnis*, vol. 8, no. 2, pp. 157–165, oct 2018.

[13] A. L. Y. A. Andrianti, "Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses DSS05 (Studi pada RS Bhayangkara Jambi)," *Indonesian Journal of Computer Science*, vol. 9, no. 2, pp. 86–95, 2020.

[14] E. Handoyo, "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST SP 800 55," *Jurnal Computer Science and Information Technology (CoSciTech)*, vol. 1, no. 2, pp. 57–64, 2020.

[15] Y. D. Imany, W. Hayuhardhika, N. Putra, and A. D. Herlambang, "Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 6, pp. 5926–5935, 2019.

[16] T. Tarwoto and A. P. Kuncoro, "Evaluasi Penerapan Sistem Informasi Smart Prodi dengan Pendekatan Delone Mclean dan Framework Cobit 5," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 18, no. 2, pp. 222–236, 2019.

[17] K. P. D. Dharmayanti, I. P. A. Swastika, and I. G. L. A. Raditya Putra, "Tata Kelola Sistem Informasi Sanken Menggunakan Framework COBIT 5," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 18, no. 1, pp. 29–38, 2018.

[18] E. Nachrowi, Yani Nurhadryani, and Heru Sukoco, "Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 4, pp. 764–774, 2020.

[19] Y. W. H. N. P. A. D. H. Rahmah, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 4, no. 3, pp. 840–847, 2020.

[20] I. Maghfiroh, M. Murahartawaty, and R. Mulyana, "Analisis dan Perancangan Tata Kelola Ti Menggunakan Cobit 4.1 Domain Deliver and Support (DS) PT XYZ," *Jurnal Sistem Informasi*, vol. 12, no. 1, pp. 50–55, 2016.

[21] N. Kadek, R. Widya, I. P. A. Bayupati, and I. K. A. Purnawan, "Audit Capability EAM Menggunakan COBIT 5 dan ISO 55002 pada Perusahaan Kelistrikan Negara," *Jurnal Merpati*, vol. 4, no. 3, pp. 195–204, 2016.

[22] K. Marzuki, A. Setyanto, and A. Nasiri, "Audit Tata Kelola Teknologi Informasi Menggunakan Cobit 4 . 1 Domain Monitoring Evaluasi Pada Perguruan Tinggi Swasta," in *Seminar Nasional Sistem Informasi dan Teknologi Informasi*, 2018, pp. 412–416.