Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13224
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Information Security Evaluation of Data Centre Architecture Using COBIT 5

Nurbojatmiko[1)] Muhammad Shidqa Irahman[2)*], Ainun Nashikha[3)], Raihan Lail Ramadhan[4)],
[1,2,3,4)]Universitas Islam Negeri Syarif Hidayatullah Jakarta
[1)]nurbojatmiko@uinjkt.ac.id,[2)]shidqa.irahman21@mhs.uinjkt.ac.id,
[3)]ainun.nashikha21@mhs.uinjkt.ac.id, [4)]raihan.lail21@mhs.uinjkt.ac.id

Submitted : Dec 10, 2023 | **Accepted** : Dec 29, 2023 | **Published** : Jan 1, 2024

Abstract: Pusat Teknologi Informasi dan Pangkalan Data (Pustipanda) UIN Jakarta is an institution in charge of managing all information systems and data management for UIN Jakarta. However, security issues are still one of the problems faced by Pustipanda today, such as data leaks, and websites that are often problematic. This research aims to assess the level of information security at the UIN Jakarta Pustipanda data centre using the COBIT 5 framework. Information security is very important in supporting organizational operations, especially facing cyber threats in the data centre environment. The research approach included document analysis, observation, and interviews with stakeholders at Pustipanda UIN Jakarta. Identification of information security weaknesses, assessment of compliance with security standards, and design of appropriate solutions are the subject of the research. It is hoped that the results will provide a comprehensive picture of information security in the data centre as well as concrete recommendations for improvement. The results of the research include an understanding of the status of information security at Pustipanda UIN Jakarta, as well as guidelines for improving information security in accordance with COBIT 5 principles. These efforts aim to reduce risk and protect the integrity, confidentiality, and availability of data in the data centre environment

Keywords: APO13; COBIT 5; Data Center; DSS05; EDM

INTRODUCTION

In today's digital era, the main challenge for companies, organisations, and governments is maintaining information system security. The existence of Information System Security is crucial in the era of Information and Communication Technology (ICT) (Ciptaningrum *et al.*, 2015). Information and data security is a major focus for various organisations, including educational institutions such as Pustipanda UIN Jakarta. Pusat Teknologi Informasi dan Pangkalan Data (Pustipanda) is an institution responsible for data and information management at UIN Syarif Hidayatullah Jakarta, which has the responsibility of managing crucial information. According to Aritonang, several problems arise, including a lack of evaluation of the maturity level of system security, a lack of response to reports, and a lack of guidelines and SOPs related to information system security policies (Aritonang *et al.*, 2018). Therefore, evaluating the security maturity of information systems is a must to ensure business continuity and efficiency today. Thus, improvements can be made to increase the level of information system security in accordance with the demands of the times).

This research aims to conduct an in-depth evaluation of information security in the data centre architecture Pusat Teknologi Informasi dan Pangkalan Data (Pustipanda) UIN Jakarta using the COBIT 5 framework. COBIT 5 is recognised as an industry standard in Information Technology governance and information security, and will be used to evaluate various aspects of information security in use

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

today as well as identify potential deficiencies that may pose risks in the data centre architecture at Pustipanda UIN Jakarta (Matin *et al.*, 2018).

In evaluating enterprise security, focus will be placed on COBIT 5 domains such as APO13 and DSS05 (Greene & CISSP, 2015). This evaluation aims to address various challenges and risks related to information security, such as differences in security policies, lack of understanding of potential risks, suboptimal governance, technology and infrastructure limitations, as well as linkages to applicable security standards and implementation. According to Tristiyanto, to find out the company's governance in managing IT infrastructure in the form of value delivery, risk optimisation, resource optimisation, it will focus on COBIT 5 Domains such as EDM01, EDM01, and EDM03 (Tristiyanto & Octaria, 2019). Through the application of the COBIT 5 framework, this research is expected to provide a comprehensive evaluation and recommendations that can be applied to strengthen information security in the data centre architecture at Pustipanda UIN Jakarta.

The results of this research are expected to assist Pustipanda UIN Jakarta in improving and maintaining information security on stored data, so as to ensure the integrity and confidentiality of critical information. In addition, the findings of this research are expected to provide valuable insights for other educational institutions and organisations facing similar challenges in maintaining and strengthening information security. In the next section, this research will describe the methodology used, key findings, and recommendations that can be applied to improve the security of the data centre architecture at Pustipanda UIN Jakarta using the COBIT 5 framework.

LITERATURE REVIEW

Data Center Architecture

A data centre is a facility used to place electronic systems and their related components for the purposes of data placement, storage, and processing (Menkominfo, 2013). Data centre can also be interpreted as a facility used to store, process, and distribute data centrally. Data centres are important assets for organisations that use information technology (IT) to support their business activities.

Data centres must have good information security to protect data from internal and external threats, such as leakage, damage, theft, sabotage, and so on. Certain data centres generally include special building structures, power backup structures, cooling systems, special rooms (such as entrances and communication rooms), device cabinets, cable structures, network devices, storage systems, servers, mainframes, software applications, physical security systems, monitoring centres, and many other supporting systems. all of these resources interact with each other and are managed by special officers (Santana, 2013).

Information Security

Information Security is the protection of information and information systems from unauthorised access, use disclosure, interference, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST, 2013). Protection of information and information systems from unauthorised access, use, disclosure, interference, modification, or destruction in order to provide confidentiality, integrity, and availability (CNSS, 2010). It can be concluded that information security is a process to ensure the confidentiality, integrity, and availability of information. Information security involves technical, organisational, and human aspects. Information security must be managed systematically and continuously to reduce risk and improve Information Technology (IT) performance.

Information security awareness is the awareness of users to comply with rules, realize potential, understand responsibilities, and act in accordance with information security (Nurbojatmiko *et al.*, 2020). Information security can be interpreted as confidentiality that protects information from unauthorized access, integrity that maintains the integrity of information from unauthorized modification, and information availability that ensures data can be accessed by authorized users.

COBIT 5

COBIT 5 is a framework used to manage and oversee IT in a holistic and integrated manner. COBIT 5 has five principles, namely:

Meeting stakeholder needs,

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

Information Technology (IT) governance is required to meet the needs and expectations of stakeholders, such as business owners, customers, employees, regulators, and others. IT governance is also expected to create value for stakeholders by optimally managing IT risks, resources, and performance.

Covering the enterprise end-to-end,
Information Technology (IT) governance covers all activities and business processes related to Information Technology, whether performed by the Information Technology function or by other business units. Information Technology (IT) governance can also integrate and align Information Technology with business strategies, objectives, and policies.

Applying a single integrated framework,
Information Technology (IT) governance uses a single, integrated framework that incorporates the best standards, practices, and methods available in the field of Information Technology. IT governance should be able to adopt and adapt the framework according to the context and needs of the organisation.

Enabling a holistic approach,
Information Technology (IT) governance uses a holistic and systemic approach that considers all factors affecting Information Technology, such as principles, policies, processes, structures, culture, ethics, information, services, infrastructure, applications, and people. Information Technology (IT) governance can be used to identify, manage, and monitor all enablers or every influencing factor in an integrated manner.

Separating governance from management,
Information Technology (IT) governance separates the governance function from the management function. The governance function is to set direction, decisions, and oversight over Information Technology, while the management function is to plan, build, run, and monitor Information Technology. Information Technology governance can also establish boundaries, responsibilities, and accountability between the two functions.

According to (ISACA, 2012) the COBIT 5 framework also has seven enablers that serve to provide a comprehensive and integrated framework for managing and controlling information technology in an organisation. The following 7 enablers in COBIT 5 are as follows Principles, policies and frameworks, Processes, Organisational structures, Culture, ethics and behaviour, Information, Services, infrastructure and applications, People, skills and competencies.

COBIT 5 can be used to evaluate data centre information security using the APO13 (Manage Security) and DSS05 (Manage Security Services) processes. The APO13 process aims to establish and maintain information security policies and procedures in accordance with business and regulatory needs. The DSS05 process aims to provide effective and efficient information security services to protect the data centre from threats (Zulhuda, 2010).

COBIT 5 is a framework specifically designed to guide organisations in managing and securing their information assets. COBIT 5 provides detailed guidance for every aspect of information security, including risk identification, resource protection, and ongoing monitoring (ISACA, 2012).

EDM (Evaluate, Direct, and Monitoring)

EDM (Evaluate, Direct, and Monitoring) is one of the domains of COBIT 5 that aims to assess, optimise risks and resources, including practices and activities to evaluate strategic options, provide direction to IT, and monitor results. EDM domain processes include: EDM01, Ensure Governance Framework Setting and Maintenance. EDM02 Ensure Benefit Delivery. EDM03, Ensure Risk Optimisation, EDM04 Ensure Resource Optimisation, and EDM05 Ensure Stakeholder Transparency (ISACA, 2012).

APO (Align, Plan, and Organize)

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

APO (Align, Plan, and Organize) is one of the domains of COBIT 5 which aims to focus on how an organisation can organize and manage information technology (IT) in line with its business objectives. This research will focus on APO13 (Manage Security) which helps companies audit information system security governance and evaluate the level of security maturity of a company's information system (Aritonang *et al.*, 2018).

DSS (Deliver, Service, Support)

DSS (Deliver, Service, Support) is one of the domains of COBIT 5 that focuses on how organisations manage the delivery, service, and support of IT services to ensure that these services can provide the expected value in accordance with business needs. This research will focus on DSS05 (Manage Security Services) which aims to find out the extent to which the company manages information system security and its conformity with the company's security policies, and monitors the company in managing and overseeing security systems (ISACA, 2012).

Capability Level

Capability level is the level of process capability that shows the extent to which the process can achieve the expected goals" (Surya *et al.*, 2021). Capability level in COBIT 5 is a measure of IT process maturity used to evaluate how well IT processes are managed and controlled. Capability level in COBIT 5 is the level of maturity or maturity of an IT process in a company/organisation. According to (ISACA, 2012), the capability level in COBIT 5 is divided into 6 levels:

Level 0: Incomplete Process

At this stage, the IT process still cannot be implemented and still cannot achieve business process goals (Tristiyanto & Octaria, 2019).

Level 1: Performed Process

At this stage, a process can already be implemented and can achieve its goals (ISACA, 2012).

Level 2: Managed Process

At this stage, the process has been managed and controlled in planning, monitoring, evaluating, and the results of the work product of the process will then be determined, controlled, and maintained (Tristiyanto & Octaria, 2019).

Level 3: Estabilished Process

At this stage, the process has been defined in detail and is based on a standardised process.

Level 4: Predictable Process

At this stage, the process is consistently enforced within specified limits (ISACA, 2012).

Level 5: Optimising Process

At this stage, the process can be improved regularly to achieve current and future business goals (Andry & Cristianto, 2018).

METHOD

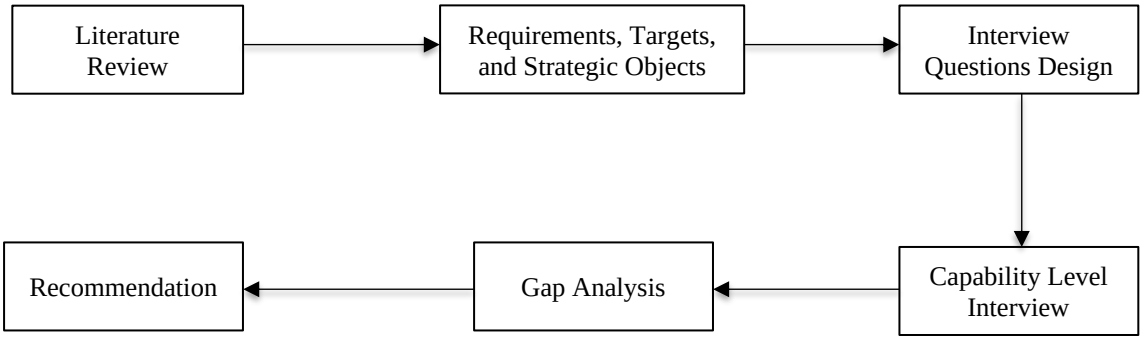

Figure 1. Research Methodology

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

Research methodology is a research plan structure consisting of plans and procedures for carrying out research, which includes general assumptions, research strategies, data collection methods, and detailed analysis (Ishtiaq, 2019). This research uses quantitative methods as a research strategy, with data collection techniques in the form of literature studies, observations, and interviews. This research also followed the stages shown in the research plan (Figure 1), namely preliminary studies consisting of literature studies and case studies. The results of this research plan are requirements, targets, and strategic objects that correspond to various processes in the EDM, DSS, and APO domains. These domains are used as the basis for developing interview questions, with reference to the COBIT 5 standard.

Question Table

The question table (Table 1) in this study was compiled to assess each domain used as a standard in evaluating information security at the Pustipanda UIN Syarif Hidayatullah Jakarta Data Center. With a total of 18 questions (3 items for domain EDM01, 2 items for domain EDM02, 2 items for domain EDM03, 6 items for domain DSS05, and 5 items for domain APO13).

Table 1. Interview Questions

Domain	Question
EDM01	1. How does pustipanda manage data centers? 2. Is there a special regulation in pustipanda in managing data centers? 3. Is the hierarchical structure of IT Governance at pustipanda in accordance with the needs of the organization in managing the data center?
EDM02	1. Is the performance of the data center able to meet business needs and objectives? 2. How efficient is the data center in resource usage?
EDM03	1. How does pustipanda identify the risks that exist in the data center? 2. How does pustipanda manage all risks in the data center system?
DSS05	1. How do you handle errors in a data center? 2. How do you manage physical access and logical access to the data center? 3. Are measures in place to minimize the business impact of operational information security vulnerabilities and incidents? 4. Can all users be uniquely identified and have access rights according to their business roles? 5. Are there physical measures in place to protect information from unauthorized access, damage and interference while being processed, stored or transmitted? 6. Is electronic information truly secure when stored, or transmitted?
APO13	1. How does pustipanda monitor data center security? 2. Is there a separate security application in pustipanda? 3. Is the security system that has been implemented in accordance with the requirements or has it been deemed appropriate for pustipanda? 4. Is there an internal pustipanda plan and communication related to system security implementation? 5. Are information system security solutions implemented in all divisions or sections in pustipanda?

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

RESULT

The results and discussion of this research are organized in tabular form consisting of 3 main tables, namely the question table, assessment results, and recommendation results.

Research Results

Table 2 shows the results of measuring the capability level of IT governance using the COBIT 5 framework. Capability level is the level of an organization's ability to perform IT processes that have been defined. in the COBIT 5 assessment model. Capability levels have a scale from 0 to 5, namely :

0 (Incomplete Process) : the IT process is not performed or does not achieve its goal.
1 (Performed Process) : the IT process is performed and achieves its objectives, but is unorganized and uncontrolled.
2 (Managed Process) : IT processes are carried out in an organized and controlled manner, but are not documented and not measurable.
3 (Established Process) : IT processes are carried out in a documented and measurable manner, and in accordance with established standards.
4 (Predictable Process) : IT processes are carried out consistently and predictably, and in accordance with the specified limits.
5 (Optimizing Process) : IT processes are optimized and can be improved, and are in line with business objectives.

Based on the average assessment in the Capability Level assessment table (Table 2), it is known that the overall average for each domain (EDM01 is 2.33; EDM02 is 2.13; EDM03 is 2; DSS05 is 3; APO13 is 1.55) tested is 2.202 (Managed Process), which explains that IT processes are carried out in an organized and controlled manner, but are not documented and not measurable.

Table 2. Capability Level Assessment For Each Domain

Domain	Capability Level (Average)	
	As Is	To Be
EDM01	2,33	4
EDM02	2,13	4
EDM03	2	4
DSS05	3	4
APO13	1,55	4

Recommendation Results

Table 3. Recommendations For Assessment Using The EDM01 Domain

EDM01 (Ensure Governance Framework Setting and Maintenance)

Existing Condition	Value	Target	Recommendation
Pustipanda already has regulations on system security, but it is still unclear and there is a lack of attention to data center security. Thus creating vulnerabilities in terms of security	2,33	4	Revise existing system security regulations in accordance with applicable security standards and more clearly. Increase attention or awareness of data center security. Conduct regular audits and evaluations of data center security, and implement control and monitoring mechanisms for access and activities in the data center.
Awareness of information security in data centers is still in the low category	1,5	4	Make information security policies and procedures that are clear, complete, and easily understood by all parties involved with the data center. As well as periodic socialization and education about

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13224
e-ISSN : 2541-2019
p-ISSN : 2541-044X

			information security to all parties involved with the data center.
There is already a hierarchical structure in the organization for data center governance.	3,16	4	Review the existing hierarchical structure, involving all parties related to the data center. Identify discrepancies in the hierarchical structure of each data center governance and the parties involved in data center governance. Create a document explaining the new hierarchical structure that is easily understood by all parties involved in data center governance.

Table 4. Recommendations For Assessment Using The EDM02 Domain

EDM02 (Ensure Benefit Delivery)			
Existing Condition	**Value**	**Target**	**Recommendation**
Performance has not been able to fulfill because there are many obstacles in procurement caused by several internal factors	1,9	4	Create and establish clear procurement standards and procedures that are easily understood by all parties involved in the procurement process. Establish and develop a competent, professional and responsible procurement team. And supervise and control the procurement process periodically and systematically.
The campus in providing support related to the procurement of costs in the data center has not been maximized.	2,16	4	Create and submit a clear and convincing procurement proposal to the campus on the impact of procurement costs for the data center. Build and maintain good and professional relationships with the campus (especially with stakeholders). And provide the value and benefits of the data center to the campus.
Use of resources is still not adequate and efficient	2,33	4	Identify and measure the resources used in the data center. Analyze and compare resource usage with set standards and targets. Plan and implement strategies to improve more adequate and efficient resource usage. Supervise and control resource usage on an ongoing basis to ensure that resource usage is in line with the objectives and needs of the data center.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13224
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 5. Recommendations For Assessment Using The EDM03 Domain

EDM03 (Ensure Risk Optimization)			
Existing Condition	**Value**	**Target**	**Recommendation**
No specific regulations for overall data security	1,16	4	Implement industry security standards such as ISO 27001, implement data encryption, strict access control, ensure effective physical security and monitoring, and establish clear security policies.
Many threats and risks will arise in information security aspects such as website security, student data security, and various other security aspects.	2,5	4	Strengthen information security by updating website software, implementing encryption for student, lecturer, and other data, using firewalls and intrusion detection, and conducting regular security audits.
Pustipanda has not yet thoroughly managed the threats and risks that arise due to lack of funds and costs.	2,33	4	Identify the most important security risks and concentrate your efforts on them. Continue to make persuasive efforts to gain support and understanding from campus leadership regarding the importance of security.

Table 6. Recommendations For Assessment Using The DSS05 Domain

DSS05 (Manage Security Services)			
Existing Condition	**Value**	**Target**	**Recommendation**
Pustipanda reads logs from the server to identify errors to fix using various tools.	3,5	4	Implement a system that can automate reading logs so that the system can immediately detect errors and provide recommendations for improvement.
Pustipanda is still not comprehensive for managing physical and non-physical access to the data center.	2,16	4	Strengthen security by increasing security personnel to manage physical access, and strengthen discipline for all security stakeholders, both physical and non-physical.
Pustipanda for security management using fingerprints, cctv, and various other types of security tools (software and hardware)	4	4	Conduct regular monitoring and maintenance of security support assets so that these assets are always available.
For data security, pustipanda uses a firewall to detect all security threats both internal and external. The firewall detects IP to identify security.	3,66	4	Strengthen the firewall system and perform maintenance on the firewall regularly.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024
DOI : https://doi.org/10.33395/sinkron.v9i1.13224
e-ISSN : 2541-2019
p-ISSN : 2541-044X

There are obstacles when updating, due to budget issues so that the update process is hampered.	2	4	Coordinate well with the faculty to procure funds so that pustipanda can update the security system regularly.
Pustipanda has a backup system when a worker is absent.	3,5	4	It is important to ensure that the type of work being backed up matches the job desc and knowledge of the replacement worker. It is important not to assign work to a busy worker so as to burden the worker.
The information stored can be ensured to be secure, but there is a bureaucracy on campus that can cause a decrease in the security of the information stored.	2,16	4	Submit a good and clear proposal to convince the campus of the importance and vitality of information security issues.

Table 7. Assessment Recommendation Using APO13 Domain

APO13 (Manage Security)			
Existing Condition	**Value**	**Target**	**Recommendation**
Pustipanda does not use a special application, because the application is paid and Pustipanda has limited budget.	1	4	Updating the latest security patches on systems and software. And implement a security layer approach using firewalls, antivirus, and other security tools.
From pustipanda, it still feels lacking for the security system, because the budget given is not maximized to get the results towards the desired goal.	1,83	4	Establish partnerships with security agencies or organizations that can provide additional support or resources without significant costs.
Pustipanda has planned to improve security implementation but has always been unable to materialize due to bureaucratic issues.	1,83	4	Improve communication between the security team and the authorities by clearly conveying the urgency and benefits of the security upgrade. Create supporting business documents or proposals to clarify the positive impact of security investments.

The recommendations given are based on making each process reach capability level 4 or Predictable Process, where the security system can be implemented stably and consistently. In the case of this research, the recommendation is the importance of procuring costs by the campus related to the security of the pustipanda data centre so that problems such as data leaks, and websites that are often problematic can be resolved, considering that the pustipanda itself already has systems and regulations for security issues, which in its application are still inconsistent due to budget constraints.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 8, Number 1, January 2024 e-ISSN : 2541-2019
DOI : https://doi.org/10.33395/sinkron.v9i1.13224 p-ISSN : 2541-044X

DISCUSSIONS

This research measures the level of IT process capability in data center information security at Pustipanda UIN Jakarta using the COBIT 5 framework and interview method. The IT processes evaluated in this study are EDM01 (Ensure Governance Framework Setting and Maintenance), EDM02 (Ensure Benefits Delivery), EDM03 (Ensure Risk Optimization), DSS05 (Manage Security Service), and APO13 (Manage Security). These processes were chosen because they represent important aspects of data center information security, namely governance framework setting, benefits delivery, risk optimization, security service management, and security management.

The results showed that the IT process is at Level 2 Managed Process, which means that the IT process is planned but not consistent. The results of this study are in line with several similar studies that have been conducted previously. For example, research conducted by Matin *et al.* (2018), who evaluated data center information security using COBIT 5 with a focus on the APO13 and DSS05 processes. which also found weaknesses and risks in data center information security. The recommendations given are to increase costs, communication, coordination, standards, procedures, analysis, services, and technology related to data center information security in order to reach Level 4 Predictable Process, which means that IT processes are stable and measurable.

CONCLUSION

The evaluation carried out on the security of the Data Center at Pustipanda UIN Jakarta was carried out using the COBIT 5 framework with the EDM, DSS, and APO domains. data collection is done by conducting interviews with related parties regarding regulations and existing conditions of data center security. Based on the evaluation results, the capability level obtained based on interviews in the EDM01, EDM02, EDM03, DSS05, and APO13 processes is 2.202, or if rounded, obtaining a capability level of Level 2 Managed Process. The recommendations given are based on making each process reach capability level 4 or Predictable Process, which is defined as a security system that can be implemented stably and consistently. In the case of this research, recommendations in the form of the importance of procuring costs by the campus related to the security of the pustipanda data center so that various problems such as data leaks, and websites that are often problematic can be resolved, considering that the pustipanda itself already has systems and regulations for security issues, in its application it is still inconsistent due to budget constraints.

REFERENCES

Andry, J. F., & Cristianto, K. (2018). *Audit Menggunakan COBIT 4.1 dan COBIT 5 Dengan Case Study*. Graha Ilmu, Teknosain.

Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13). *ITEJ (Information Technology Engineering Journals)*, *3*(2), 6–10. https://doi.org/10.24235/itej.v3i2.27

Ciptaningrum, D., Nugroho, E., & Adhipta, D. (2015). Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5. *Sentika*, *2015*(Sentika), 6.

Committee on National Security Systems (CNSS). (2010). *National Information Assurance (IA) glossary*. The National Security Systems Instruction, (4009), 103.

Greene, F., & CISSP. (2015). *Selected COBIT 5 Processes for Essential Enterprise Security*. ISACA.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. USA: ISACA.

Ishtiaq, M. (2019). Book Review Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (4th ed.). Thousand Oaks, CA: Sage. *English Language*

*name of corresponding author

Teaching, *12*(5), 40. https://doi.org/10.5539/elt.v12n5p40

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2018). Analisis Keamanan Informasi Data Center Menggunakan Cobit 5. *Jurnal Teknik Informatika*, *10*(2), 119–128. https://doi.org/10.15408/jti.v10i2.7026

Menkominfo. (2013). *Peraturan Menteri Komunikasi dan Informatika Republik Indonesia: Pedoman Teknis Pusat Data*. *53*(9), 1689–1699.

NIST. (2013). NISTIR 7298 Revision 2, National Institute of Standards and Technology. NIST IR, 7298(2), 222. https://doi.org/10.6028/NIST.IR.7298r3

Nurbojatmiko, Fajar Firmansyah, A., Aini, Q., Saehudin, A., & Amsariah, S. (2020). Information Security Awareness of Students on Academic Information System Using Kruger Approach. *2020 8th International Conference on Cyber and IT Service Management*, CITSM 2020. https://doi.org/10.1109/CITSM50537.2020.9268795

Santana, G. A. A. (2013). *Data Center Virtualization Fundamentals: Understanding Techniques and Designs for Highly Efficient Data Centers with Cisco Nexus, UCS, MDS, and Beyondtle*. Cisco Press.

Surya, S. D., Khairan, A., Ahmad, M. S., Sirajuddin, H. K., & Zainuddin. (2021). Information of Technology Service Governance Capability Level Audit on Khairun Ternate University (Case Study, System Information of Kubermas). *E3S Web of Conferences*, *328*, 1–7. https://doi.org/10.1051/e3sconf/202132804004

Tristiyanto, & Octaria, C. (2019). IT Governance Audit at Lampung University Using COBIT 5 Framework Focus on EDM Domain. *Journal of Physics: Conference Series*, 1338(1). https://doi.org/10.1088/1742-6596/1338/1/012060

Zulhuda, S. (2010). Information security in the Islamic perspective: The principles and practices. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World: ICT Connecting Cultures*, ICT4M 2010. https://doi.org/10.1109/ICT4M.2010.5971936

*name of corresponding author