Asia Pacific Journal of Information System and Digital Transformation
2023, Vol 1 No 01, Research Article

Data Security Management and Audit of Healthcare Data: A Case Study of SISPEC19 Project

Nurul Wahda R. Kasad
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
nurulwahdark@student.telkomuniversity.ac.id

Deden Witarsyah Jacob
Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia
dedenw@telkomuniversity.ac.id

Ramdhan Nugraha
Department of IT Convergence Engineering, Kumoh National Institute of Technology
ramdhan@kumoh.ac.kr

Abstract

Data security is the biggest challenge with personal data and state secrets threats. Digital transformation is increasing in various industries, including the government industry. One of the causes of this is the Covid19 pandemic which imposes conditions where all activities can be carried out smoothly even though they cannot interact directly. In this study, an analysis was carried out regarding auditing and data security management on health data in a government-owned health information system using the DAMA-DMBOK approach as a data governance standard. Then an audit is carried out to measure the success rate of implementing security on information systems using COBIT 2019 as a standard for IT governance.

Keywords: DAMA, Security, Data, Control.

1. Introduction

Data is the core asset for creating decisions in an organization, community, or government (GAUTAM & BHIMAVARAPU, 2022). The data shows collection facts from any activity or process that already record and saved into the current media. So that the data will continue to evolve, some roles of the organization have their every data needs to create a strategy and planning for the organization's future sustainability. While the COVID-19 pandemic has many impacts, such as implementing digital transformation to optimize government decisions when taking the best solution (ACTIAN, n.d.). For example, a software, platform, or application can use to know about the update of vaccination data, how many people are yet to get the vaccine,

vaccine dose even deliver education about Covid-19. The organization needs data to serve this, but if the data quality isn't accurate, not synchronized, loss, and free to modification will influence when analyzing it. Data is the main basic information technology that has several vulnerabilities to manipulation.

SISPEC19 as a web application based platform that provides the update of vaccination data, people's data who are yet to get the vaccine, covid-19 patient, covid-19 announcement, and education about covid-19. One of the sensitive data that is used such as identity cards of people. SISPEC19 managed by some roles in government like public health center, hospital, party administering the vaccination and the government itself. However, within the implementation, the data security of Sispec19 was never tested, so there are many potential threats of the sensitive data. It's about data access and permission.

Based on these problems, it is necessary to develop a data security management appropriate to the situation. One of the standards that can use is data security management based on DAMA-DMBOK Framework. DAMA-DMBOK is a data governance framework that has standards for data management processes, clearly, consistently to be a reference (Henderson, Cupoli, & Earley, 2014).

2. Conceptual Background

2.1 Data Security Management

Data security Management is a way to protect the data by using some principles and standards for preventing such as unauthorized, manipulation, and loss the data (Giri & Shakya, 2019). Data security management is a strategy that aims to keep the data quality, integrity, confidentiality, and availability of the data (Bertino & Ferrari, 2017). The main purpose of data security management is ensuring data access, permission, authentication well managed (Kumar, Raj, & Jelciana, 2018). While the benefit of data security management such as keep the data performance stability, the application performance, build a trust of users who needs the data, the data privacy, and give the biggest implication within make decision for the government.

There are several tools that must be attention to optimize the security management of data (ACTIAN, n.d.):

- Planning and governance tools for monitoring data throughout its lifecycle.
- Know what data that has and why.
- Data integrity verification.

- Understand where the information is stored and under what circumstances.
- Make sure the data is erased if necessary.

2.2 Data Governance

Data governance is a standard for evaluation specifically in data management (Atlan Pte. Ltd., 2022). The evaluation of this management process starts from matters related to the initialization of roles and responsibilities related to the parties involved in the management process itself, actions that need to be taken by the current and future conditions of the organization, and its needs related to the management process of data and information technology itself. (Henriques, Almeida, Pereira, Silva, & S. Bianchi, 2020). In data governance, the management process carried out aims to maintain the quality and accuracy of the data as well as its accountability. For this reason, data management has several principles including (Janssen, Brous, Estevez, S. Barbosa, & Janowski, 2020):

- Evaluate the quality of the data and matters related to the data
- Detect changes to data
- Distribute data as needed
- Give appreciation to the actors of data analysis
- Prioritize transparency when distributing data
- Separate personal and/or sensitive data from non-personal and/or non-sensitive data
- Give the user the right to check the accuracy of the data held
- Collecting data and its sources
- Apply authorization for data access
- Carry out the data merging process with permission
- Establish accountability of the data manager
- Inform data manager accountability to avoid data misuse
- Data as a valuable asset that can be used on BDAS (Big Data Algorithm Systems.

In its application, several data governance frameworks can be used according to the needs of each organization, in which the framework presented is in the form of a data management structure. Several known data governance frameworks (Atlan, 2022) :

- DAMA DMBOK (Data Management Association and Data Management Body of Knowledge). A framework from DAMA International that has the purpose of promoting the understanding, development, and practice of managing data and information as key enterprise assets to support the organization (DAMA International,

n.d.)

- The DGI (Data Governance Institute). A framework that has a logical structure for classifying, organizing, and communicating complex activities involved in making decisions about and taking action on enterprise data (The Data Governance Institute, n.d.).
- McKinsey. A framework as a research tool that considers the multifaceted nature of an organization, i.e., the organizational, team, and individual levels (Chmielewska, Stokwiszewski, Markowska, & Hermanowski, 2022).
- Eckerson. A framework that has six layers and consists of 39 components at the most granular level. As part of modernizing data governance, each element must be addressed. The structure for analyzing needs and prioritizing and sequencing modernization projects and activities (Wells, 2019).
- PwC (PricewaterhouseCoopers), A framework that pursues holistic, structured approaches and solutions while also considering individual requirements covers all processes, from generation and validation to protecting and processing the data (PwC, n.d.).

2.3 IT Governance

IT governance is defined as the management and organizational structures, processes, and related mechanisms that ensure that an organization's IT supports and enforces its strategy and goals (Haes & Grembergen, 2004). IT governance ensures that the IT department's planned ongoing actions align with the organization's business strategy and prioritize critical business needs. These demands must be met on time, at an agreed cost, and in line with requirements and quality. Then the costs and risks must be properly managed to achieve the expected benefits (Abdollahbeigi & Salehi, 2020). In the implementation, IT governance requires a framework to guide information technology management. One of the frameworks is COBIT. COBIT (Control Objective for Information and related Technology) helps companies manage their information and technology (Atrinawati, et al., 2021). Corporate information and technology refer to all information technology and processes companies apply, not just technical and information departments. ISACA has released the latest version of COBIT, namely COBIT 2019. COBIT 2019 is considered more flexible and open to various references, making it easier for users to expand their focus on information technology management. COBIT 2019 is an evolution of the previous framework, recognizing that it can be

implemented in different organizational areas. The authoritative framework for IT governance ties IT performance to business performance through business value creation, which states that value creation optimizes risk while driving optimal resource costing (Fortin & Héroux, 2018).

2.4 DAMA Internasional Framework

The DAMA (Data Management Association) Framework is one of several well-known data governance frameworks. The DAMA Framework is also a reference in the data management process in DMBOK (Prasetyo, Djepapu, Tridalestari, & Hariman, 2019). The DAMA Framework is also known as the International DAMA, where this framework supports the management of data management processes such as the creation, transformation, and transmission of data that can produce information as needed (Kanika, Emamjome, & Hofstede, 2021). The following is a model of the International DAMA.

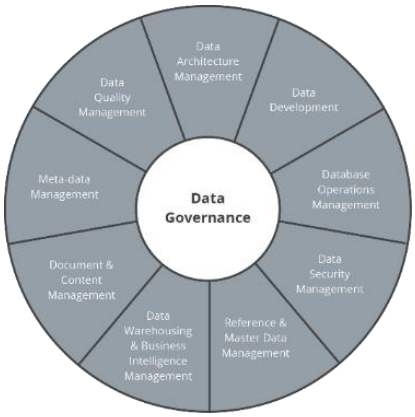

Figure 1 DAMA-DMBOK Knowledge Area

There are 10 areas contained in the International DAMA model that will be used as a reference in designing the data governance structure in this study (Henderson, Cupoli, & Earley, 2014):

1) Data Governance, fungsinya meliputi perencanaan, proses penyediaan dan manajemen kontrol serta pemanfaatan data
2) Data Architecture Management, focusing on enterprise application integration.
3) Data Development, its functions include analysis, design, testing and development, distribution, and maintenance of data.
4) Database Operations Management, which focuses on supporting the physical structure of data, defines data recovery and performance-related needs, and improves services.
5) Data Security Management, ensuring privacy, authority, and access rights.
6) Reference & Master Data Management, managing the main versions and data replicas,

ensuring the process of creating, changing, and deleting code and data references, defining requirements, and identifying problems from master data management.

7) Data Warehousing & Business Intelligence Management, providing several open access rights to be used as decision support based on data in reports and analysis.
8) Document & Content Management, managing storage, protection, indexes, and permissions for unstructured data. Create and manage metadata, define metadata access and integration requirements and use metadata to make data management and decisions more effective.
9) Meta Data Management, controlling and distributing metadata
10) Data Quality Management, defining, controlling, and improving data quality.

2.5 Data Security Management on DAMA-DMBOK

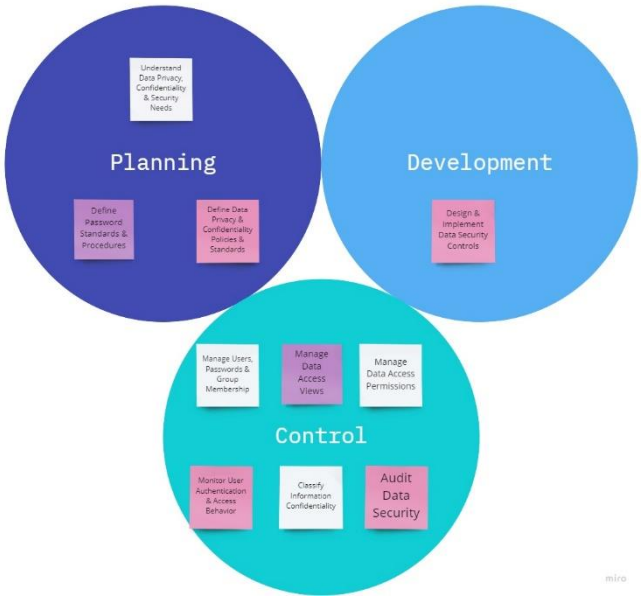

Figure 2 Data Security Management DAMA-DMBOK

1) Planning is activities that determine the strategic and tactical data management activities. Planning activities can be carried out periodically.
2) Development is activities that create a testing, model design, and deployment.
3) Control is ongoing oversight activities such as data access, audit process, and information confidentiality classification.

3. Research Methodology

There are several steps that will be carried out in this research :

1. Literature review. Collect information through several journals, articles and books relevant to research to serve as a basic guideline.
2. Collect data. Collect the data by conducting interviews with the source person regarding the implementation of data security used.
3. Identify the problems. Identify the problem based on the data.
4. Observation, making observations by mapping each problem point and determining the potential solutions given.
5. Analyze, analyzing the results of observations by adjusting each problem and the appropriate solution.
6. Creating/Improving model design, creating/improving the design of the data security topology model to serve as a proposed solution to the problems found.
7. Model design result, is the output of the design that has been made in two diagrams for each required data security management.
8. Control result, is the output of the control that has been made by COBIT 2019.

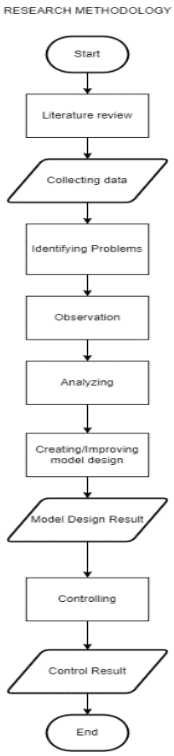

Figure 3 Research method

4. Analysis and Development of Data Security Management

4.1 Planning

Defining the security standards for the data that appropriate with data security management

requirement. The security standards that can be applied is HIPAA (Health Insurance Portability and Accountability) (HIPAA, n.d.).

Figure 4 HIPAA Security Standard

4.2 Development

A. Usecase Diagram

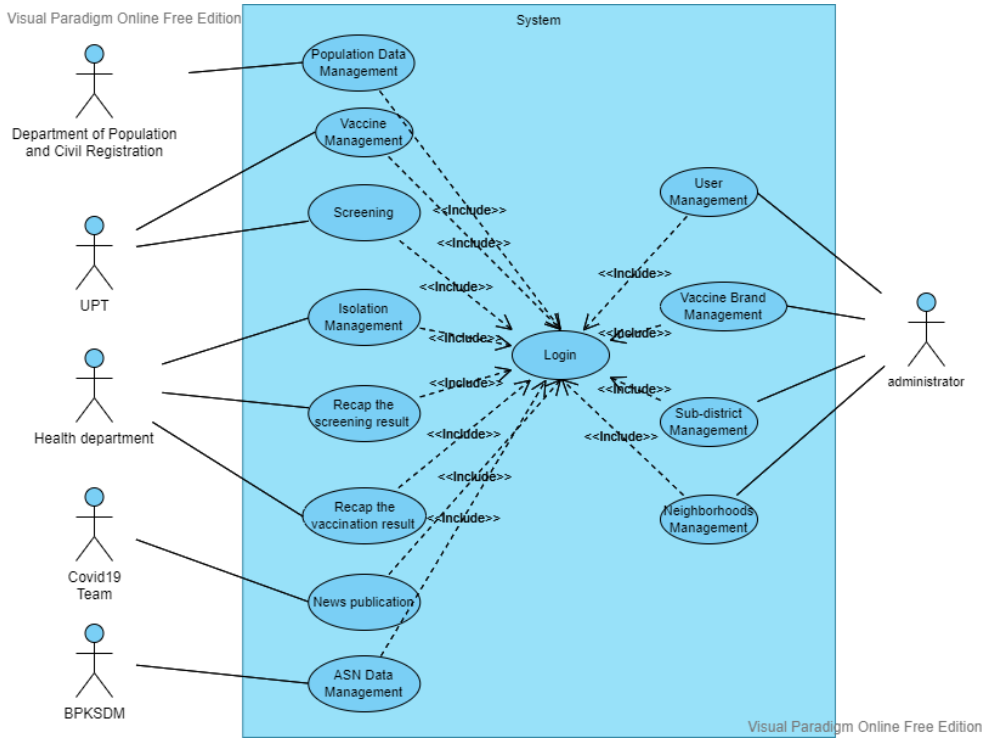

Figure 5 Usecase Diagram

B. Class Diagram

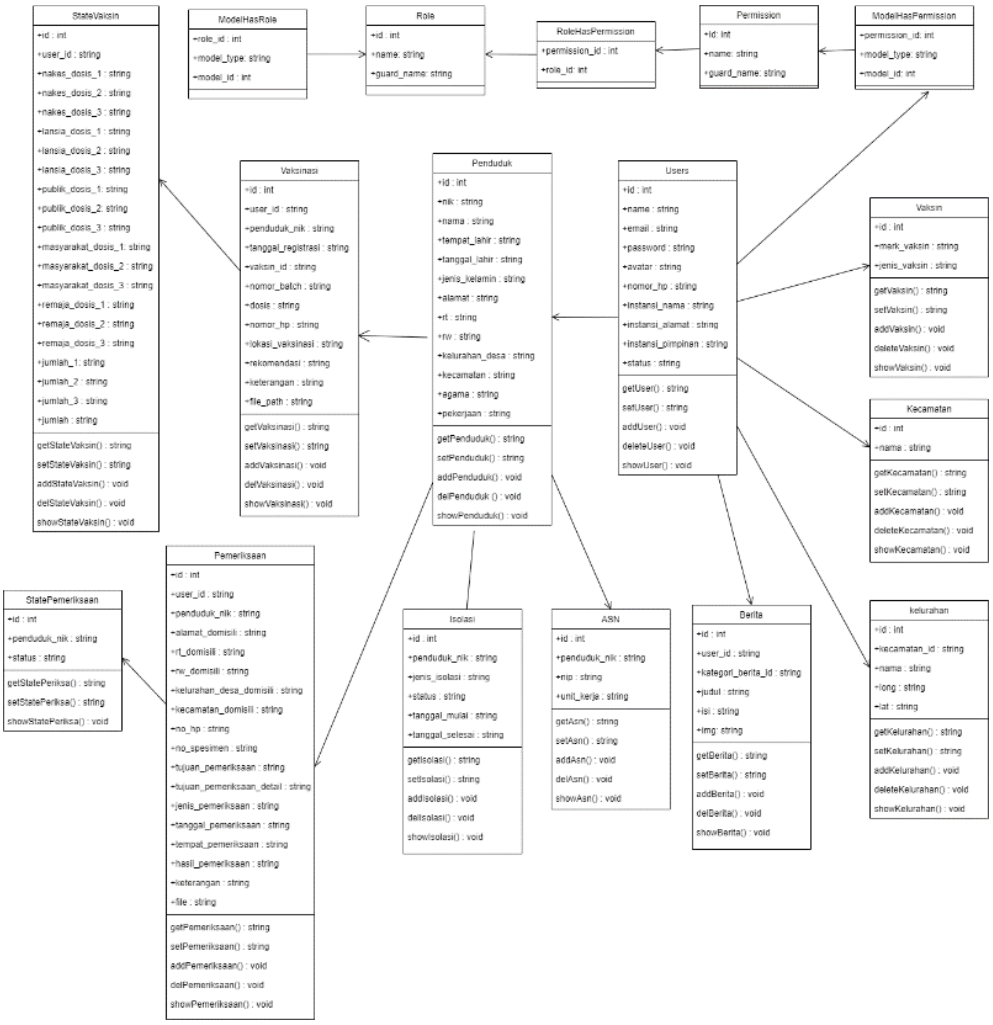

Figure 6 Class Diagram

C. Relational Database

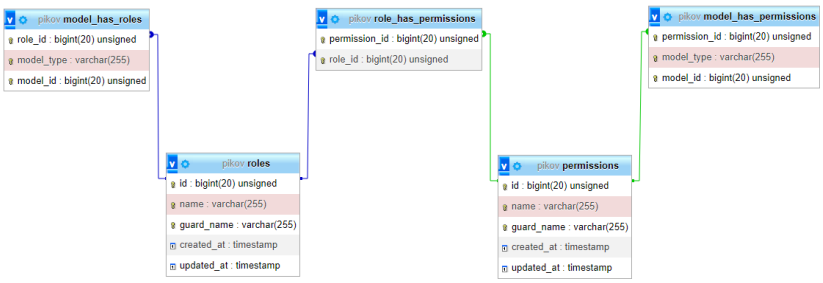

Figure 7 Relational Database

4.3 Control

A. Data Access

After previously analyzing SISPEC19, a vulnerability was found, namely port 3306 of MySQL, which was open. The existence of this vulnerability has the potential to pose a threat to the data contained in the application. These threats include data damage, loss, misuse, and so on. So, in this case, a security protocol is needed as a quality benchmark that needs to be applied. The security protocol includes IAAA (Identification, Authentication, Authorization, Accounting)-**cantumkansumber**.

1) Identification & Authentication

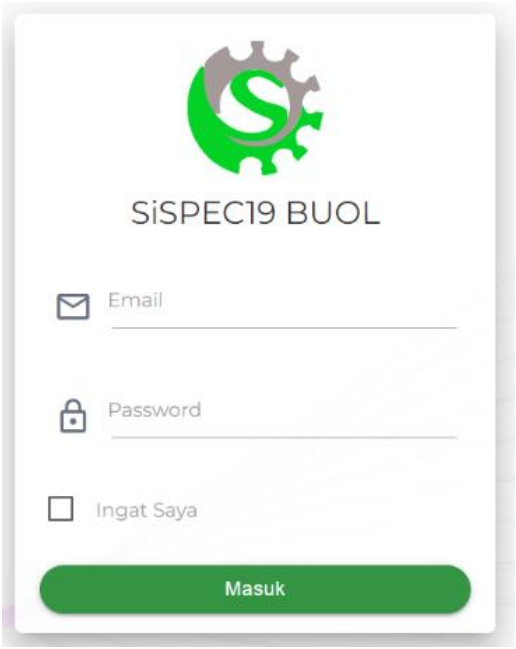

Figure 8 Login

A login form represented the implementation of identification & authentication in this project. Every user must enter their username and password, which an administrator has registered to obtain permission. Identifications are username and password. Then, authentication was represented by the password that shows appropriation with the database as a confirmation shape.

2) Authorization

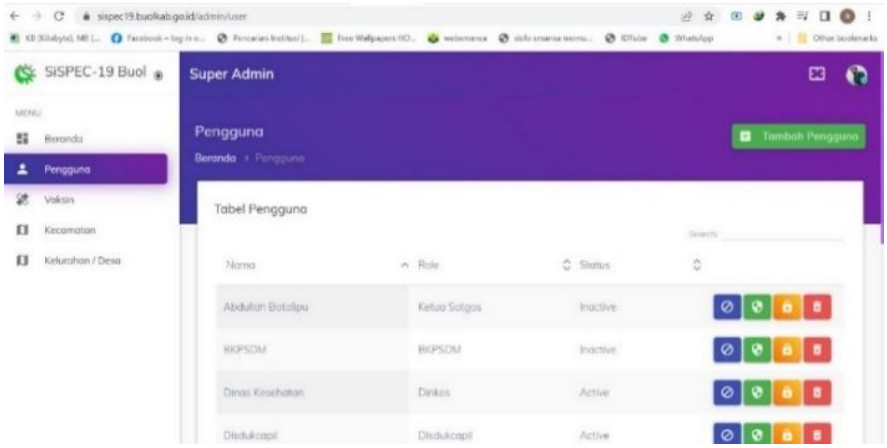

Figure 9 User Management

SISPEC19 has a feature for managing every role. It only provides admin roles. Administrators can assign the positions and all the appropriate data with the Role Based Access Control (RBAC) level. Administrators also have the privilege of knowing users who are active or inactive.

3) Accounting

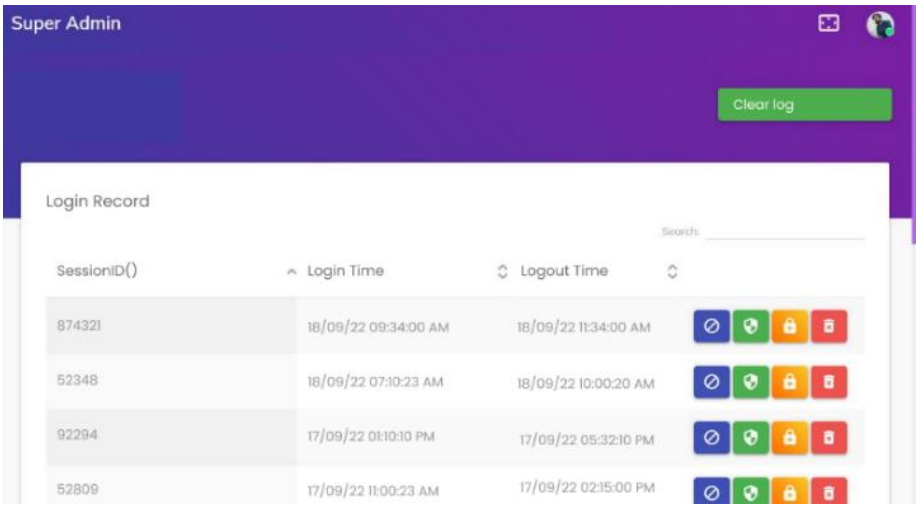

Figure 10 User Record

The administrator also can monitor the login activity of SISPEC19. Who is login in or logout. It was identified by SessionID() automatically generated from SISPEC19. This record can fulfil of Accounting aspect as the security protocols.

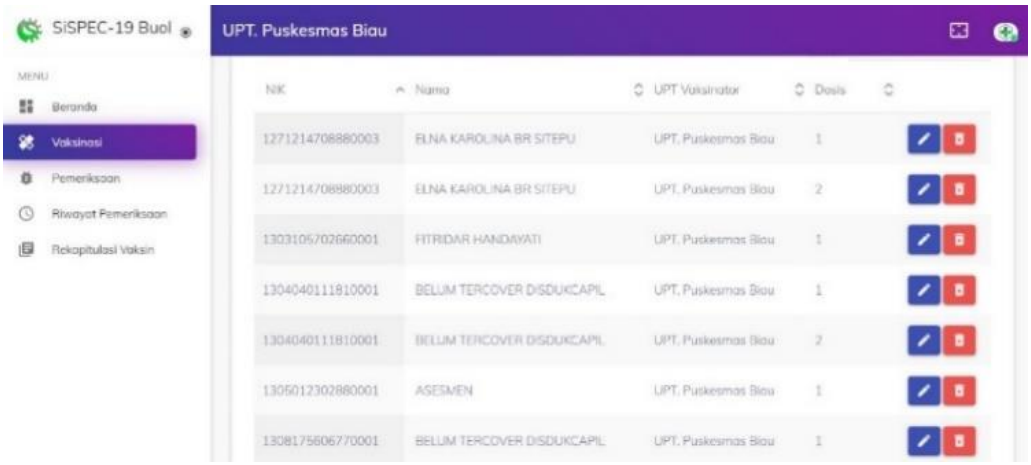

Figure 11 UPT Page and Data Access

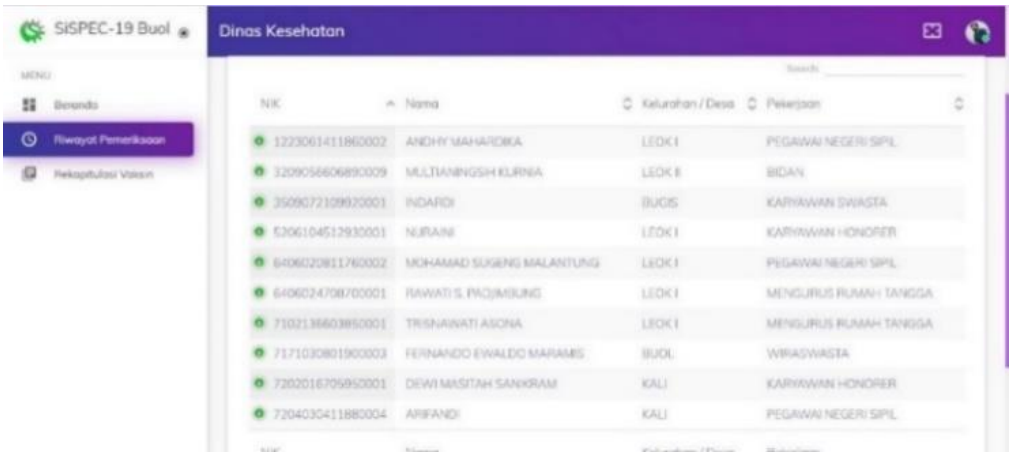

Figure 12 Health Department Page and Data Access

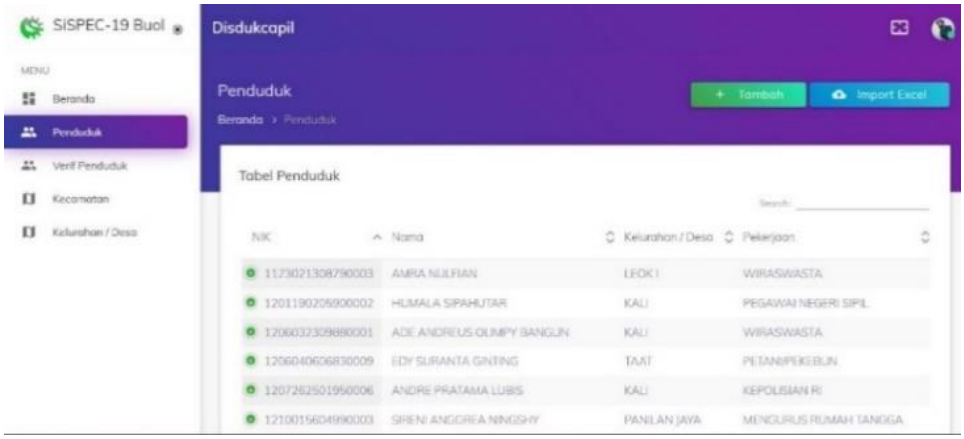

Figure 13 Department of Population and Civil Registration Page and Data Access

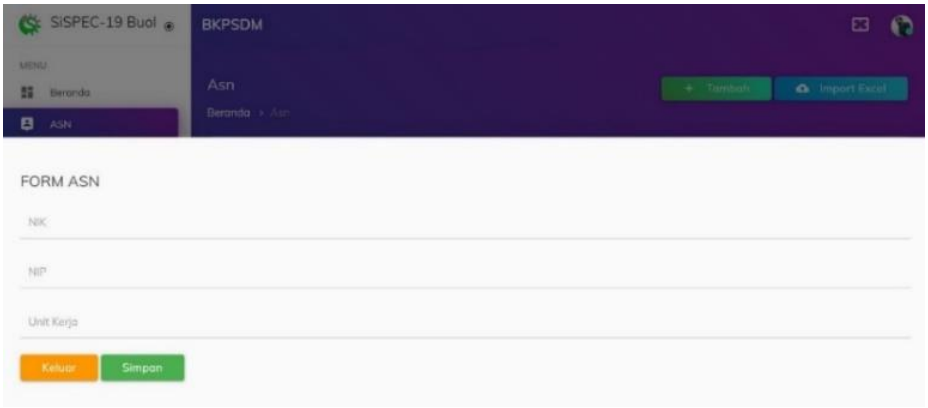

Figure 14 BPKSDM Page and Data Access

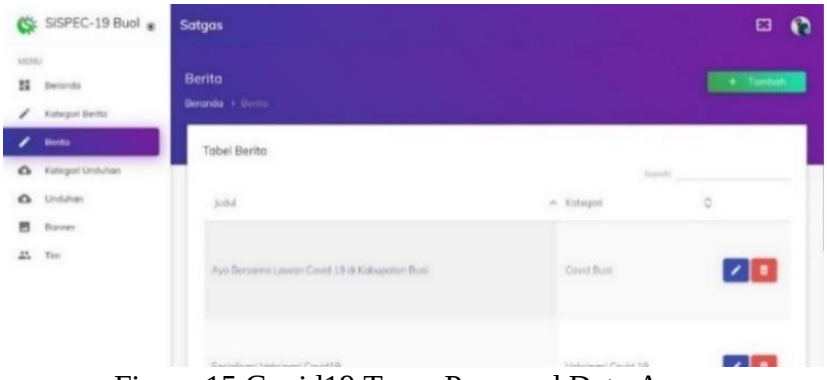

Figure 15 Covid19 Team Page and Data Access

Data Security Audit Using COBIT 2019

In conducting a security audit on this research project, COBIT 2019 was used. With its domain, DSS05, which has a management practice focused on measuring security (ISACA, 2018). The range of levels for measuring the conformity of process implementation in COBIT 2019 is (0 – 5) (ISACA, 2018). Level 0 is the lowest measurement result where the organization still needs a fundamental approach related to achieving the goals. Level 5 indicates that the processes implemented by the organization are primarily appropriate and ready to focus on managing the sustainability of the life cycle to face challenges in the future.

Table 1 DSS05.01

DSS05.01 Protect against malicious software.				
Activities	**Description**	**Answer**	**Score**	**Capability Level**
1	Install and activate malicious software protection tools on all processing facilities, with malicious software definition files that are updated as required (automatically or semi-automatically).	Partially	0,5	2
2	Filter incoming traffic, such as email and downloads, to protect against unsolicited information (e.g., spyware, phishing emails).	Yes	1	
	% Fulfillment of Level 2		75%	*Stop Here!*
3	Communicate malicious software awareness and enforce prevention procedures and responsibilities. Conduct periodic training about malware in email and Internet usage. Train users to not open, but report, suspicious emails and to not install shared or unapproved software.	No	0	3
4	Distribute all protection software centrally (version and patch-level) using centralized configuration and IT change management.	No	0	
	% Fulfillment of Level 3		0%	*Stop Here!*
5	Regularly review and evaluate information on new potential threats (e.g., reviewing vendors' products and services security advisories).	No	0	4
	% Fulfillment of Level 4		0%	*Stop Here!*

Analysis:

Based on the audit results, in Management practice DSS05.01, information system security does not install and activate malicious software protection tools yet on all processing facilities with a capability level of 2 with one activity achieved.

Table 2 DSS05.02

DSS05.02 Manage network and connectivity security.				
Activities	**Description**	**Answer**	**Score**	**Capability Level**
1	Allow only authorized devices to have access to corporate information and the enterprise network. Configure these devices to force password entry.	Yes	1	2
2	Implement network filtering mechanisms, such as firewalls and intrusion detection software. Enforce appropriate policies to control inbound and outbound traffic.	Yes	1	
3	Apply approved security protocols to network connectivity.	Partially	0,5	
4	Configure network equipment in a secure manner.	Partially	0,5	
% Fulfillment of Level 2			75%	*Stop Here!*
5	Encrypt information in transit according to its classification.	No	0	3
6	Based on risk assessments and business requirements, establish and maintain a policy for security of connectivity.	No	0	
7	Establish trusted mechanisms to support the secure transmission and receipt of information.	No	0	
% Fulfillment of Level 3			0%	*Stop Here!*
8	Carry out periodic penetration testing to determine adequacy of network protection.	No	0	4
9	Carry out periodic testing of system security to determine adequacy of system protection.	No	0	
% Fulfillment of Level 4			0%	*Stop Here!*

Analysis:

The results of the audit show that in the DSS05.02 Management practice, information system security has implemented an authorization system, filtered network connections, implemented

security protocols, and the appropriate security configuration process.

Table 3 DSS05.04

Table 4 DSS05.04 *DSS05.04 Manage user identity and logical access.*

Activities	Description	Answer	Score	Capability Level
1	Maintain user access rights in accordance with business function, process requirements and security policies. Align the management of identities and access rights to the defined roles and responsibilities, based on least-privilege, need-to-have and need-to-know principles.	Yes	1	2
	% Fulfillment of Level 2		100%	*Continue!*
2	Administer all changes to access rights (creation, modifications and deletions) in a timely manner based only on approved and documented transactions authorized by designated management individuals.	Yes	1	3
3	Segregate, reduce to the minimum number necessary and actively manage privileged user accounts. Ensure monitoring on all activity on these accounts.	Partially	0,5	
4	Uniquely identify all information processing activities by functional roles. Coordinate with business units to ensure that all roles are consistently defined, including roles that are defined by the business itself within business process applications.	Yes	1	
5	Authenticate all access to information assets based on the individual's role or business rules. Coordinate with business units that manage authentication within applications used in business processes to ensure that authentication controls have been properly administered.	Yes	1	
	% Fulfillment of Level 3		90%	*Continue!*
7	Maintain an audit trail of access to information depending upon its sensitivity and regulatory requirements.	No	0	4
8	Perform regular management review of all accounts and related privileges.	Yes	1	
	% Fulfillment of Level 4		50%	*Stop Here!*

Analysis:

Based on the audit results, in Management practice DSS05.04, the information system can manage the roles of users according to their business processes to ensure that user activities can be identified uniquely. However, knowing detailed user activities still needs to be more appropriate, so the capability level is 3 with six activity achievements.

Table 5 DSS05.06

DSS05.06 Manage sensitive documents and output devices				
Activities	**Description**	**Answer**	**Score**	**Capability Level**
1	Establish procedures to govern the receipt, use, removal and disposal of sensitive documents and output devices into, within, and outside of the enterprise.	Yes	1	2
2	Ensure cryptographic controls are in place to protect sensitive electronically stored information.	No	0	
	% Fulfillment of Level 2		50%	*Stop Here!*
3	Assign access privileges to sensitive documents and output devices based on the least-privilege principle, balancing risk and business requirements.	No	0	3
4	Establish an inventory of sensitive documents and output devices, and conduct regular reconciliations.	No	0	
5	Establish appropriate physical safeguards over sensitive documents.	No	0	
	% Fulfillment of Level 3		0%	*Stop Here!*

Analysis:

Based on the audit results, in Management practice DSS05.06, the information system has implemented procedures for classifying documents: confidential and general information. However, publishing the record has yet to be encrypted, so the capability level achieved is still at level 2 with the achievement of one activity.

Table 6 DSS05.07

DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.				
Activities	**Description**	**Answer**	**Score**	**Capability Level**
1	Continually use a portfolio of supported technologies, services and assets (e.g., vulnerability scanners, fuzzers and sniffers, protocol analyzers) to identify information security vulnerabilities.	Partially	0,5	2
2	Define and communicate risk scenarios, so they can be easily recognized, and the likelihood and impact understood.	Yes	1	
3	Regularly review the event logs for potential incidents.	Yes	1	
4	Ensure that security--related incident tickets are created in a timely manner when monitoring identifies potential incidents.	Yes	1	
% Fulfillment of Level 2			88%	*Complete!*
5	Log security-related events and retain records for appropriate period.	No	0	3
% Fulfillment of Level 3			0%	*Stop Here!*

Based on the audit results, in Management practice DSS05.07, the information system has defined risk scenarios, has a recording process as material for incident management and ensures timeliness in handling incidents. However, the capability level that can be achieved is still at level 2 with four activity achievements because the activity in scanning the vulnerabilities in the system has yet to be entirely carried out correctly.

5. Conclusion

Based on the discussion, it can be concluded that:

a. DAMA-DMBOK approach can support data governance mechanisms within the information system of government.
b. Information systems built previously are analyzed in terms of security using the DAMA-DMBOK standard. It is because the information system used as an application in the government stores a myriad of nationally sensitive population identity data.
c. So that information systems can be used safely and support government programs following data governance standards.

References

1. Abdollahbeigi, B., & Salehi, F. (2020). THE CRITICAL FACTORS IF IT GOVERNANCE AND ITS IMPACT. 81-99.
2. ACTIAN. (n.d.). *Data Management*. Retrieved December 2022, 30, from https://www.actian.com/what-is-data-security-management/
3. Atlan. (2022, December 9). *What is a Data Governance Framework and How Can You Create One for Your Organization?* Retrieved December 12, 2022, from https://atlan.com/data-governance-framework/
4. Atlan Pte. Ltd. (2022, September 29). *6 Commonly Referenced Data Governance Frameworks in 2022 and Why Your Organization Needs One*. Retrieved from atlan: https://atlan.com/data-governance-framework/
5. Atrinawati, L., Ramadhan, E., Fiqar, T., Wiranti, Y., Abdullah, A., Saputra, H., & Tandirau, D. (2021). Assessment of Process Capability Level in University XYZ Based on COBIT 2019.
6. Bertino, E., & Ferrari, E. (2017). Big Data Security and Privacy. *31*, 425-439.
7. Chmielewska, M., Stokwiszewski, J., Markowska, J., & Hermanowski, T. (2022). Evaluating Organizational Performance of Public Hospitals using the McKinsey 7-S Health Framework. *BMC Health Services Research*(7).
8. DAMA International. (n.d.). *About >> Mission, Vision, Purpose, and Goals*. Retrieved January 2, 2023, from https://www.dama.org/cpages/mission-vision-purpose-and-goals
9. Fortin, A., & Héroux, S. (2018). The moderating role of IT-business alignment in the relationship between IT governance, IT competence, and innovation. *Information System Management*, 98-123.
10. GAUTAM, R. S., & BHIMAVARAPU, V. M. (2022). Data Driven Decision Making: Application in Finance. *5*(12).
11. Giri, S., & Shakya, S. (2019). E-government Use in Nepal: Issues of Database Management and Data Security. *15*(2).
12. Haes, S., & Grembergen, W. (2004). IT Governance and Its Mechanisms. *INFORMATION SYSTEMS CONTROL JOURNAL, 1*.
13. Henderson, D., Cupoli, P., & Earley, S. (2014). DAMA-DMBOK2 Framework. In *DAMA International.*
14. Henriques, D., Almeida, R., Pereira, R., Silva, M. M., & S. Bianchi, I. (2020). How IT Governance can assist IoT project implementation. *8*(3), 25-45.
15. HIPAA. (n.d.). *HIPAA Academy*. Retrieved January 1, 2023, from https://hipaaacademy.net/hipaa-security-rule/
16. ISACA. (2018). *COBIT® 2019 FRAMEWORK: GOVERNANCE AND MANAGEMENT OBJECTIVES.*
17. Janssen, M., Brous, P., Estevez, E., S. Barbosa, L., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence.
18. Kanika, G., Emamjome, F., & Hofstede, A. (2021). Data governance for managing data quality in process mining.
19. Kumar, P., Raj, P., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. 691–697.
20. Prasetyo, H. N., Djepapu, R. N., Tridalestari, F. A., & Hariman, I. (2019). Development of Project Document Management System Based on Data Governance With DAMA International Framework. *2*.

21. PwC. (n.d.). *Data management*. Retrieved January 1, 2023, from https://www.pwc.de/en/finance-transformation/data-management.html
22. The Data Governance Institute. (n.d.). *We know Data Governance*. Retrieved January 1, 2023, from https://datagovernance.com/
23. Wells, D. (2019, August 14). *The Path to Modern Data Governance*. (Eckerson Group) Retrieved January 2, 2023, from https://www.eckerson.com/articles/modern-data-governance-problems

DOI: https://doi.org/10.61973/apjisdt.v101.4