PULMONOLOGY

Audit of Hospital Management Information Systems in Public Healthcare Institutions: A Clinical Governance Perspective

Dr. Thabo Maseko[1]*, Dr. Naledi Khumalo[1]
[1]Department of Health Informatics, Chris Hani Baragwanath Academic Hospital, Johannesburg, South Africa

ABSTRACT

Sistem Informasi Manajemen Daerah (SIMDA) is a system that was developed to assist accountability achievement in local government. The aim of this study is to audit the application area management performance information system implemented by government agencies in Tanjungpinang, Kepri. Descriptive approach was used to present an outline of the assets inventory in SIMDA. Data collection methods consist of primary data obtained from interviews and observations. As for secondary data, we used literature studies to support this study. The audit process was used the OCTAVE Allegro approach to analysis important assets owned by the government and manage risk to achieve the ISO 27001 standard. In addition, this research used five of eight steps on OCTAVE Allegro to establish the areas of concern in SIMDA application. The results presented an indication of the data discrepancy between the project proposed data and project data in SIMDA. Lack of user attention in SIMDA checking data before adding or deleting the data caused that indication. The conclusion is by determining areas of concern, it can be used as a mapping of risk to information assets while minimizing the risk as a measure to maintain the information security system of SIMDA. This study was conducted to discuss information security, SIMDA, OCTAVE Allegro, and ISO 27001.

Keyword: Audit, Information System, SIMDA, OCTAVE Allegro.

INTRODUCTION

Information security threats have increased every year along with the development of information technology (Siponen et al., 2014). With the rapid development of technology, it triggers security gaps and performance disruptions in the system in terms of information processing and networks (Liu et al., 2011). Most of the security problems caused by inappropriate use of information technology and user negligence (Chatterjee et al., 2015). Handling system security risks is a complex process that requires the role of technology in minimizing threats and increasing resilience in the system (Feng et al., 2014). The awareness of users in organizations or government agencies also has a big influence on risk management on information security (Jufri et al., 2018). By increasing user awareness of the importance of

information system security, users will strive to maintain and optimize system performance while preventing indications of information leakage (Cox, 2012).

Sistem Informasi Manajemen Daerah (SIMDA) is a system developed by Badan Pengawasan Keuangan dan Pembangunan (BPKP) in 2003 (Wahyuni, 2011). The use of SIMDA aims to achieve accountability for local governments in regional financial management (Nugraha and Astuti, 2013). To achieve this goal, the role of information system security is needed to secure information from various threats and prevent the leakage of important information belonging to local governments.

The implementation of SIMDA in Tanjungpinang City Government in general has a very strategic and vital function. SIMDA is used to collect, process data on assets and assets belonging to the region, as well as issue reports. With the importance of the regional management information system for the Tanjungpinang City Government as a form of asset inventory, it is necessary to have an audit of the SIMDA that has been running. This is considered necessary in order to find out whether the performance of SIMDA has been running effectively and efficiently. The problems that arise during the use of the SIMDA application are experiencing problems in data import and export, the results of the reports do not appear. There are frequent differences in data such as the difficulty of correcting reports because reports are in one database. SIMDA financial data management is considered complicated for users, and database sometimes experiences an error.

Financial management at Nganjuk District Health Office by relying on SIMDA Finance is considered to be quite good. With the SIMDA Finance application, it will produce financial reports and other financial information with better quality, accuracy, and timeliness. The weakness of the Financial SIMDA lies in the bookkeeping function that has not been implemented optimally and has a complicated procedure for correcting data errors in Surat Perintah Pencairan Dana (SP2D) (Nugraha and Astuti, 2013).

The use of SIMDA Barang Milik Daerah (SIMDA BMD) in Majene Regency has a significant impact in terms of effectiveness, efficiency, and decision making. It cannot be separated from the support of the government in realizing the management of the regional property in an accurate and accountable manner. Budget limitations in efforts to increase human resources, access to applications only rely on Local Area Network (LAN), and lack of coordination and communication between stakeholders are obstacles to maximizing the use of SIMDA BMD (Mahayuddin and Fatimah, 2016).

The audit process using the OCTAVE Allegro framework makes it possible to identify assets that are considered potentially threatened (Gutandjala et al., 2019) by protecting information based on risk decision-making based on the CIA (Confidentiality, Integrity, Authentication). OCTAVE Allegro makes it possible for auditors to carry out risk analysis and evaluation of the security of a system individually with the scope of assets and information within the organization (Sardjono and Cholik, 2018).

This study aims to audit the performance of SIMDA application at Tanjungpinang City Government, especially in the Dinas Pekerjaan Umum Perumahan Rakyat (PUPR) Office. This research method used a descriptive method (Colorafi and Evans, 2016).

RESEARCH METHOD

The series of research stages carried out included observation and data collection techniques based on primary and secondary data, data processing and analysis, and research

results. This research was conducted in the working area of the Tanjungpinang City Government which focuses on Dinas Pekerjaan Umum Perumahan Rakyat (PUPR). This research was conducted with an estimated research time of 3 months starting from January to March 2020, which is presented in Table 1 as follows:

Table 1. Research schedule

No.	Activities	Time
1	Determination of the research theme	January 13-17
2	Data collection	January 21-24
3	Data processing and analysis	January 27 - February 13
4	Advisory lecturer consultation	February 15 – 28
5	URL of Community Services Report	March 1 – 20

In terms of data collection, secondary data sources were obtained from literature reviews by reviewing national and international research journals. Meanwhile, primary data sources were obtained from interviews and observation techniques. The Secretary of the PUPR Office is used as a resource or informant because it has an important role in accessing information, has adequate competence, and readiness to become a resource. Interviews were conducted by asking a number of questions related to the SIMDA application. The interview questions are presented in Table 2 as follows:

Table 2. List of Interview Questions

No.	Question
1	Has the regional financial management at the PUPR Office used the application?
2	What types of applications are applied to the PUPR Office?
3	How is the SIMDA application management at the PUPR Office?

The initial stage of processing interview data is to make a transcript of all the observations and interviews that have been carried out. Transcripts are written descriptions made in detail and complete relating to the content of the conversation directly and the results of the recordings. After making the transcript is complete, transcript analysis can be carried out. This analysis was conducted to find the inherent and hidden meaning of the interview results. From the results of the transcript analysis, the next process is mapping the analysis into the framework by adjusting the stages in OCTAVE Allegro.

Operationally Critical Threat, Assets, and Vulnerability Evaluation (OCTAVE) is a methodology for identifying risk assets that potentially threatened in an organization (Gutandjala et al., 2019). In OCTAVE, there are three different methodologies, namely the OCTAVE, OCTAVE-S, and OCTAVE Allegro methods (Suroso et al.,018). OCTAVE used in large-scale organizations and has the ability for internal security evaluation (Wagiu et al., 2019). OCTAVE-S is for small-scale organizations and generally requires a collaborative risk management team (Moyo et al., 2013). In addition, OCTAVE Allegro has a scope of data and information assets that support individuals in conducting security evaluations (Sardjono and Cholik, 2018). ISO 27001 is an independent information technology standardization (Septian and Pamuji, 2019), a risk-based management approach, and information asset security

(Lenawati et al., 2017, Susanto and Shobariah, 2016). The stages in OCTAVE Allegro are shown in Figure 1.

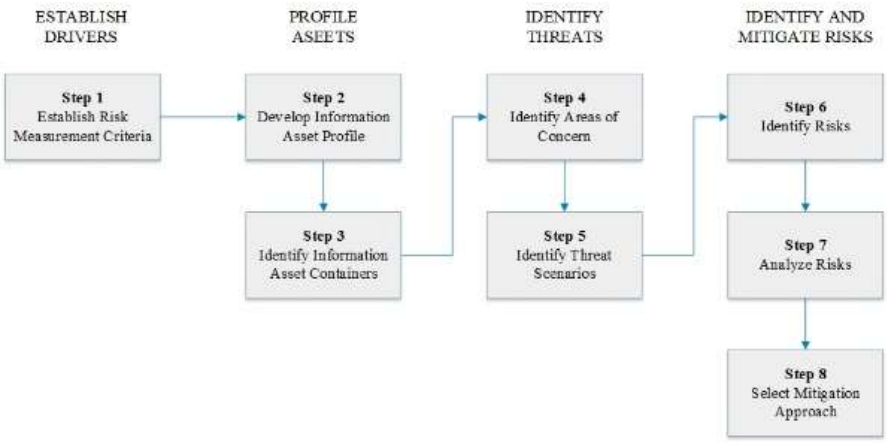

Figure 1. OCTAVE Allegro Street Map

RESEARCH RESULTS AND DISCUSSION

3.1 Results Research

The use of SIMDA can intensify local governments in implementing regional autonomy. In this study, the implementation of OCTAVE Allegro uses 5 out of 8 steps starting from establishing risk measurement criteria to identifying threat scenarios. All data in this session were obtained from the results of interviews which were used as analysis material for each stage in OCTAVE Allegro. The explanation of the research results using the 5 steps of OCTAVE Allegro is shown in Table 3 below:

Table 3. OCTAVE Allegro Mapping Results

No.	Description	Results
1	Step 1 Determine risk measurement criteria	The financial sector, regional property (BMD), and productivity.
2	Step 2 Define the information asset profile	Important assets which include planning, budgeting, purchasing, administration, and reporting
3	Step 3 Identify media information assets	Media categories are technical, physical, and user.
4	Step 4 Identification of special areas	Areas of particular concern are data differences in SIMDA and the database having errors
5	Step 5 Identify threat scenarios	Identify a threat profile that includes information assets, actors, means, motives, results, and security requirements.

The results of this study found that there were differences in project data on the SIMDA application. These results serve as areas of concern due to gaps in the system. However, previous research revealed that the audit results obtained were incoming notifications by the

AIS administration and threats of infiltration (Jufri et al., 2018). The spread of access rights (passwords) to online system applications and the use of security holes in online system applications can be included as areas of concern (Wagiu et al., 2019).

DISCUSSION

In the initial step, the determination of risk measurement criteria is an important step for classifying the impact areas from various sectors. The comparison of the mapping results is shown in Table 4 as follows:

Table 4. OCTAVE Allegro's Step 1 Comparison

Research by the author	Jufri Research (MT Jufri, M. Hendayun, and T. Suharto, 2018).	Wagiu Research (EB Wagiu, R. Siregar, and R. Maulany, 2019)
Impact Area: **Finance** **BMD** **Productivity**	**Impact Area:** Reputation Belief Finance Productivity Security Penalty	**Impact Area:** Reputation Belief Finance Security Penalty
Equation: The impact area has similarities in the financial sector and productivity.		
Difference: In impact area, there are differences in the sector of reputation and trust, security, and punishment		

After determining the impact area, the next step is to determine the priority scale based on the impact area. Determination of the priority scale is sorted from the existing scale values in the impact area. The more important the impact area, the greater the priority scale value. The priority scale in this study is sorted from productivity scale 1, finance scale 2, and regional property (BMD) scale 3. Based on the priority scale above, research by Jufri has a priority scale, namely security and safety on scale 1, fines and penalties on scale 2, productivity on scale 3, finance on scale 4, reputation and trust. scale 5 (Jufri et al., 2018). Determining an asset profile requires some information about the critical asset that will be identified in the critical asset information worksheet. The comparison of the mapping results is shown in Table 5 as follows:

Table 5. OCTAVE Allegro's Step 2 Comparison

Research by the author	Jufri Research (MT Jufri, M. Hendayun, and T. Suharto, 2018).	Wagiu Research (EB Wagiu, R. Siregar, and R. Maulany, 2019)
Asset: **- Item plan** **Maintenance**	**Asset:** Budget - Acquisition of assets	**Asset:** Financial Information - Employee information

Budget **- Acquisition of assets** **- Accounting documents** **- Deposit documents REPORTING**	- Deposit documents REPORTING - AIS Database	Appraisal Attendances
Equation: There are similarities in critical assets including a budget, asset procurement, deposit documents, and reporting**.**		
Difference: There are differences in assets that are considered important including goods planning, maintenance, accounting documents, data databases, financial and employee information, appraisal, and attendance.		

To identify information media assets, it is necessary to have information storage and information asset delivery processes that can be divided into three categories including technical, physical, and people. Technical is a mechanism using technology as the main support for the system. Physical is the location for managing internal documents belonging to the organization. People are internal and external parties to the organization who have access rights to documents or information. The comparison of the mapping results is shown in Table 6 as follows:

Table 6. OCTAVE Allegro's Step 3 Comparison

Research by the author	**Jufri Research (MT Jufri, M. Hendayun, and T. Suharto, 2018).**	**(EB Wagiu, R. Siregar, and R. Maulany, 2019)**
Technical: **- Database** **- Hardware** **- Software** **Physical:** **Server** **Workspaces** **People:** **4 operational staff.**	**Internal:** - Database Server **External:** List of biblical names starting with A - System division	**Internal:** - Database - online system application **External:** List of biblical names starting with A
Equation: **From the results of the identification of information media assets have the same in the database, server, and admin.**		
Difference: **Asset information media also has differences, including hardware, software, workspace, system division, and online system applications.**		

The determination of the area of concern can be identified with a comprehensive description of the actual conditions that impact on information assets in government agencies. The comparison of the mapping results is shown in Table 7. In addition, it identifies threat scenarios by fully describing the threat profile which includes actors, intentions, motives,

outcomes, and security requirements. The comparison of the mapping results is shown in Table 8.

Table 7. OCTAVE Allegro's Step 4 Comparison

Research by the author	Jufri Research (MT Jufri, M. Hendayun, and T. Suharto, 2018).	Wagiu Research (EB Wagiu, R. Siregar, and R. Maulany, 2019)
Area of concern: The difference in data in SIMDA, and database experiences errors	**Area of concern:** Login access notifications, threats of intrusion, database experienced the error, and employees connected to computer networks using third-party applications	**Area of concern:** Staff can enter malicious code, spread access rights freely, system modules can be accessed by outsiders, and exploit online system application security holes.
Equation: In the area of concern, there is only 1 similarity, namely, the database sometimes experiences an error.		
Difference: The difference in the area of concern can be seen from differences in SIMDA data, login access notifications, threats of intrusion, use of third party applications, malicious code, distribution of access rights, and utilization of application security holes.		

Table 8. OCTAVE Allegro's Step 5 Comparison

Research by the author **- Threat Scenarios:** The identification of threat scenarios is carried out on the procurement project data assets with the areas of concern where there are data differences between the proposed project and the actual project data. This scenario contains actors of PUPR Dinas staff who make mistakes in project data due to not being serious about checking project data before adding or deleting data. This results in the modification and loss of important data. From this scenario, a solution is obtained by adding validation and verification when adding or removing.
(MT Jufri, M. Hendayun, and T. Suharto, 2018). **- Threat Scenarios:** Identify threat scenarios on AIS Database assets of which *areas of concern* focus on login access notifications. The role of AIS Administrator staff as actors with a motive that unauthorized people can access, add or delete system data. The result has an impact on data modification and asset destruction. The precautionary measure given is to make policies in managing system login access by users.
(EB Wagiu, R. Siregar, and R. Maulany, 2019) **- Threat Scenarios:** There is no threat scenario because this research only implements 4 steps of OCTAVE Allegro

CONCLUSION

From the results above, the conclusion is that the use of SIMDA in Tanjungpinang City Government, especially at the PUPR Office, has had a significant impact both in terms of effectiveness and efficiency. Reports from SIMDA can be used as a basis for decision making to achieve organizational goals and objectives as stated in the Strategic Plan. To manage this risk, it is necessary to improve the system security conditions in the SIMDA application and encourage the active participation of PUPR employees in information security. The author hopes that the development of the SIMDA application by BPKP can be the best solution in fixing problems and weaknesses in the system. The results of this study are expected to contribute to the PUPR Office in the form of guidelines in managing asset risk in the SIMDA application. This research has not achieved maximum results due to the limited time given by the campus in conducting research during the COVID-19 pandemic, and limited supporting resources which include asset data information and closed information storage media. It is expected that there will be developments for the future by perfecting the 3 advanced stages of OCTAVE Allegro, which is currently being analyzed until stage 5, namely identification of threat scenarios. The advanced stages include risk identification, risk analysis, and selection of mitigation approaches.

BIBLIOGRAPHY

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. Journal of Management Information Systems, 31(4), 49-87.

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. HERD: Health Environments Research & Design Journal, 9(4), 16-25.

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior, 28(5), 1849-1858.

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Information sciences, 256, 57-73.

Gutandjala, I. I., Gui, A., Maryam, S., & Mariani, V. (2019, August). Information System Risk Assessment And Management (Study Case at XYZ University). In 2019 International Conference on Information Management and Technology (ICIMTech) (Vol. 1, pp. 602-607). IEEE.

Jufri, M. T., Hendayun, M., & Suharto, T. (2017, November). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. In 2017 Second International Conference on Informatics and Computing (ICIC) (pp. 1-6). IEEE.

Lenawati, M., & Winarno, W. W. (2017). Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. Speed-Sentra Penelitian Engineering dan Edukasi, 9(1).

Liu, H., Cheng, Y., Yang, Z., & Zhang, Z. (2011, August). Research on security testing of information system based on interface communication. In Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology (Vol. 8, pp. 3915-3918). IEEE.

Moyo, M., Abdullah, H., & Nienaber, R. C. (2013). Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems (pp. 1-6). IEEE.

Nugraha, H. A., & Astuti, Y. W. (2013). Analisis Penerapan Sistem Informasi Manajemen Keuangan Daerah (SIMDA Keuangan) dalam Pengolahan Data Keuangan pada Organisasi Pemerintah Daerah (Studi Kasus pada Dinas Kesehatan Kabupaten Nganjuk). Jurnal Akuntansi Aktual, 2(1), 25-33.

Sardjono, W., & Cholik, M. I. (2018, September). Information Systems Risk Analysis Using OCTAVE Allegro Method Based at Deutsche Bank. In 2018 International Conference on Information Management and Technology (ICIMTech) (pp. 38-42). IEEE.

Septian, R. F., & Pamuji, G. C. (2019, November). Risk Analysis of Dutch Healthcare Company Information System. In IOP Conference Series: Materials Science and Engineering (Vol. 662, No. 2, p. 022041). IOP Publishing.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224.

Sultan, M., & Fatimah, J. M. (2017). Evaluasi Sistem Informasi Manajeman Barang Milik Daerah (Simda-bmd) dalam Mendukung Inventarisasi Aset Daerah di. KAREBA: Jurnal Ilmu Komunikasi, 5(1), 118-129.

Suroso, J. S., & Rahaju, S. M. N. (2018, October). Evaluation Of IS Risk Management Using Octave Allegro In Education Division. In 2018 International Conference on Orange Technologies (ICOT) (pp. 1-8). IEEE.

Susanto, A., & Shobariah, E. (2016, April). Assessment of ISMS based on standard ISO/IEC 27001: 2013 at DISKOMINFO Depok City. In 2016 4th International Conference on Cyber and IT Service Management (pp. 1-6). IEEE.

Wagiu, E. B., Siregar, R., & Maulany, R. (2019, December). Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method. In Abstract Proceedings International Scholars Conference (Vol. 7, No. 1, pp. 1741-1750).

Wahyuni, T. (2011). Uji empiris model delone dan mclean terhadap kesuksesan sistem informasi manajemen daerah (SIMDA). Jurnal BPPK: Badan Pendidikan Dan Pelatihan Keuangan, 2, 12-12.