Journal of Medical Records and Information Technology (JOMRIT)

Vol.3, No. 2, December 2025,
ISSN: XXX-XXXX,

Information Security Assessment of Hospital Management Information Systems Using the COBIT 2019 Framework: A Case Study of Semen Padang Hospital

Rury Moryanda[1], Herman Susilo[1], M. Syahputra[1]
[1]Universitas Syedza Saintika, Padang, Sumatera Barat, Indonesia

Article Info

Article history:

Received October 23, 2025
Revised November 12, 2025
Accepted December 30, 2025

Keywords:

COBIT 2019
Information System Security Audit
Risk Management (EDM03, APO12, APO13)
Security Controls (WAF, IDS/IPS, Penetration Testing)
ISO 27001 Compliance

ABSTRACT

This study examine the implementation of information systems at Semen Padang Hospital, focusing on improving information system security. The audit was conducted using the COBIT 2019 framework, covering the domains and processes EDM03, APO12, and APO13. The research involves risk identification, determination of security controls, and ensuring compliance with the standards set by COBIT 2019. The findings indicate that the current information system security level is at Level 2, with a gap of two-level below thw wxpected state. Therefore, improvements and enhancements to information security at Semen Padang Hospital are required. The steps taken include implementation security techniques such as vulnerability scanning, penetration testing, the use of Web Application Firewall, Intrusion Detection System, Intrusion Prevention System and data encryption. Enhancing physical security of servers, including CCTV installation and access control using cards or fingerprints, security certifications like ISO 27001 to ensure compliance with security standards. Employee training to enhance understanding and capabilities in dealing eith security threats and to strengthen coordination among staff. The measures aim to improves the hospital's system security and ensure ongoing compliance with relevant security standards.

Corresponding Author:

Rury Moryanda
Program Studi Manajemen Informasi Kesehatan, Universitas Syedza Saintika
Jl. Prof. Dr. Hamka No. 228 Air Tawar Timur, Padang, Sumatera Barat, Indonesia
E-mail: rurymorzz@gmail.com

1. INTRODUCTION

Hospitals are healthcare institutions that provide medical services through the utilization of various facilities, technologies, and professional personnel. As vital components of the healthcare system, hospitals are required to continuously adapt to societal and technological developments, particularly in the adoption of information technology. The implementation of information technology has become a key indicator of healthcare modernization, as it enhances operational efficiency, reduces costs, and improves the quality and standards of patient care [1].

One of the major forms of information technology adoption in hospitals is the Hospital Management Information System (HMIS). HMIS is designed to manage, store, process, and analyze patient health data, as well as to support both clinical and managerial decision-making across multiple hospital departments [2]. This system integrates various applications, including medical information systems, laboratory systems, radiology, pharmacy, and other service units, thereby creating a structured and continuous flow of information.

Semen Padang Hospital, a non-governmental Class C hospital managed by the PT Semen Padang Foundation, has implemented an integrated computerized information system since 2013. The hospital is committed to providing high-quality services to the community through the development of information systems that support service effectiveness. The HMIS was developed to meet operational needs, improve service efficiency, and simplify administrative processes related to patient services, information management, accounting, and procurement [3].

However, the utilization of information technology also introduces new risks to data security, such as cyberattacks, data breaches, and malware dissemination. Therefore, systematic and comprehensive security measures are required through structured security audits. Information system security evaluation in hospitals involves the examination and assessment of systems and implemented security controls to ensure that patient data are protected from both internal and external threats [4]. Information security is a critical aspect, as system disruptions can directly affect hospital operations and the quality of healthcare services.

The rapid development of information technology in the healthcare sector has positioned information systems as the backbone of hospital service management. The implementation of HMIS enables real-time integration of medical and administrative information flows, thereby supporting faster, more accurate, and more reliable clinical decision-making. Nevertheless, this technological adoption also presents serious challenges, particularly in the area of information security. Several studies indicate that the majority of security incidents in hospitals are associated with failures in information security risk management, including unauthorized access and data theft, which negatively affect patient privacy and institutional reputation [5][6][7]. Consequently, an effective information security system is essential to ensure data reliability and protection in hospital operations.

As one of the leading healthcare providers in West Sumatra, Semen Padang Hospital faces challenges in ensuring that its HMIS remains secure and compliant with applicable regulations. The implementation of HMIS in this hospital must also align with national and international standards to guarantee service quality and information security. Based on preliminary observations, several weaknesses in security risk management remain, including the lack of regular security audits and limited security awareness training for staff. These conditions pose significant security risks, particularly in the face of increasingly complex and structured cyber threats.

Control Objectives for Information and Related Technology (COBIT) 2019 is a comprehensive and integrated framework for information technology governance and management that aims to help organizations achieve strategic objectives through optimal utilization of information technology. In the hospital context, COBIT 2019 serves as a guideline for conducting information security audits, including risk identification and evaluation, determination of required security controls, and assurance of compliance with established standards and regulations [8]. By implementing security audits based on the COBIT 2019 framework, hospitals are expected to enhance information security levels, strengthen risk management, and ensure sustainable operations and continuous service quality.

2. METHOD

2.1 Type of Research

This study employs a quantitative descriptive research design aimed at providing an overview of the information system security level of the Hospital Management Information System (HMIS) at Semen Padang Hospital based on the COBIT 2019 framework. A quantitative approach is used to determine the capability level of information security management through the relevant processes defined in COBIT 2019.

2.2 Research Variables

This study involves two main variables: hospital management information system security as the independent variable, and information system security process capability as the dependent variable. The capability is measured based on the COBIT 2019 domains and processes, namely EDM03 (Ensure Risk

Optimization/Information Security Risk Management), APO12 (Risk Management), and APO13 (Security Management).

2.3 Data Collection

Data were collected using a questionnaire distributed to respondents to assess the security capability of the HMIS in accordance with the COBIT 2019 domains. The questionnaire employed a 5-point Likert scale to measure the level of understanding and implementation of each process.

2.4 Research Informants

The informants involved in this study consisted of personnel responsible for information system security management at Semen Padang Hospital. The inclusion criteria were staff members working in the HMIS unit who are directly involved in information security management, have a minimum of one year of experience in HMIS management or information security, and are willing to participate in the study. The exclusion criteria included staff who are not involved in HMIS management or maintenance activities, as well as newly recruited staff or those with less than one year of service in the HMIS unit.

2.5 Research Instrument

The primary research instrument was a 5-point Likert scale questionnaire consisting of statements related to the capability of each COBIT 2019 process. Respondents were asked to rate each statement on a scale from 1 to 5, with the following scoring categories:
1 = strongly disagree,
2 = disagree,
3 = agree,
4 = strongly agree,
5 = very strongly agree.
The resulting scores were used to calculate process capability levels and to identify gaps between the current condition (“as-is”) and the expected condition (“to-be”).

2.6 Data Analysis

Data analysis was conducted in several stages. First, questionnaire data were processed and analyzed to obtain the average scores for each security process using the Likert scale, representing the capability levels of each domain (EDM03, APO12, and APO13) according to the COBIT 2019 framework. Subsequently, a process activity rating was performed for each information security domain, where capability levels were assessed and compared with the standard or ideal condition (“to-be”) to identify gaps (gap analysis). This gap analysis aimed to determine discrepancies between the current condition (“as-is”) and the expected condition (“to-be”). When gaps were identified, root cause analysis and improvement recommendations were formulated. Conclusions were drawn based on the gap analysis results; significant gaps indicate potential weaknesses in HMIS security. In addition, the relationship between the capability level of each domain and HMIS security was analyzed to determine the extent to which each process supports effective information security risk management.

2.7 Validity and Reliability Testing

To ensure the validity and reliability of the questionnaire, validity and reliability tests were conducted using a representative pilot sample consisting of HMIS staff at Semen Padang Hospital. The validity test results showed that all questionnaire items were valid, with validity coefficients ranging from 0.562 to 0.804. The reliability test yielded a Cronbach’s Alpha value of 0.856, indicating a high level of internal consistency of the instrument.

3. RESULTS AND DISCUSSION

3.1 RACI Analysis

RACI analysis is a project management tool used to define the roles, responsibilities, and involvement of each member within a team or organization. This analysis was applied to the EDM and APO domains as presented in Table 1.

Table 1. RACI Mapping for EDM and APO Domains

Key Management Practices	Director	General Manager of Maintennce	General Manager IA & QA	Geberal Manager of

				Information System
EDM03.01	✓	✓	✓	
EDM03.02	✓	✓	✓	
EDM03.03	✓	✓	✓	
APO12.01	✓	✓	✓	✓
APO12.02	✓	✓	✓	✓
APO12.03	✓	✓	✓	✓
APO12.04	✓	✓	✓	✓
APO12.05	✓	✓	✓	✓
APO12.06	✓	✓	✓	✓
APO13.01	✓	✓	✓	✓
APO13.02	✓	✓	✓	✓
APO13.03	✓	✓	✓	✓

Based on the RACI analysis, it can be concluded that the Information Systems Unit of Semen Padang Hospital plays a central role in ensuring information system security within the hospital. This conclusion is supported by the high number of responsible (R) roles assigned to this unit in the RACI mapping, indicating its primary responsibility in information security management.

3.2 Rating of Process Activities

The capability level was determined based on the assessment of process activities obtained from questionnaire data completed by respondents. This evaluation was used to measure how well the implementation of procedures within the COBIT 2019 framework achieves defined objectives and meets established control standards.

Table 2. Rating of Process Activities – EDM03

Proses	Level 1	Level 2	Level 3	Level 4	Level 5
Score		97,22%	60%		
Achievement Scale		F	L		
Capability			Level 3		

Keterangan: N (*Not Achieved*, 0%-15%), P (*Partially Achieved*, >15%-50%), L (*Largely Achieved*, >50%=85%), F (*Fully Achieved*, >85%-100%)

Based on Table 2, the EDM03 process (Ensuring Information Security Risk Management) reached Capability Level 3 (Defined) with an activity achievement score of 60%. However, several implementation constraints were identified, including the lack of continuous monitoring and updating of the risk profile, suboptimal system evaluation, absence of structured risk analysis implementation, lack of security certification, and inadequate security monitoring methods and techniques.

Table 3. Rating of Process Activities – APO12

Proses	Level 1	Level 2	Level 3	Level 4	Level 5
Score		72%			
Achievement Scale		L			
Capability		Level 2			

Keterangan: N (*Not Achieved*, 0%-15%), P (*Partially Achieved*, >15%-50%), L (*Largely Achieved*, >50%=85%), F (*Fully Achieved*, >85%-100%)

Based on Table 3, the APO12 process (Risk Management) achieved Capability Level 2 with an activity achievement percentage of 72%. Nevertheless, several obstacles were identified, including the absence of structured documentation of risk incident history (or documentation not being systematically classified and not aligned with industry standards), and the lack of regular updates to IT risk scenarios.

Table 4. Rating of Process Activities – APO13

Process	Level 1	Level 2	Level 3	Level 4	Level 5
Score		73,08%			
Achievement Scale		L			
Capability		Level 2			
Keterangan: N (*Not Achieved*, 0%-15%), P (*Partially Achieved*, >15%-50%), L (*Largely Achieved*, >50%=85%), F (*Fully Achieved*, >85%-100%)					

Based on Table 4, the APO13 process (Managed Security) achieved Capability Level 2 with an activity achievement percentage of 73.08%. However, implementation barriers were also identified, including the absence of structured documentation of risk incident records, or where documentation exists, it is not systematically classified and not aligned with applicable industry standards. In addition, IT risk scenarios have not been updated regularly.

3.3 Gap Analysis

Within the COBIT 2019 framework, gap analysis is defined as a comparison process between the current condition ("as-is") and the expected condition ("to-be"). The purpose of this analysis is to identify discrepancies between existing conditions and predefined standards or targets.

Table 5. Gap Analysis Results

Process	*As is*	*To be*	*Gap*
EDM03	3	4	1
APO12	2	4	2
APO13	2	4	2

The gap analysis results indicate that the HMIS information security capability at Semen Padang Hospital is currently at Level 2, and has not yet achieved the desired Level 4. This gap demonstrates that the existing capability level remains below the expected standard, indicating the need for systematic improvement in information security governance and management.

3.4 Discussion

Semen Padang Hospital needs to strengthen its information security strategy through comprehensive risk evaluation and the continuous implementation of both technical and managerial measures. This approach aligns with studies emphasizing the importance of risk management in maintaining information security. Research by [9] highlights that effective information security management must address risks holistically, focusing on data protection, information accuracy, and resource availability, which are fundamental to organizational operations, particularly in high-risk sectors such as healthcare.

In the EDM03 domain (Ensuring Information Security Risk Management), Semen Padang Hospital is required to update its risk profile and implement structured risk analysis using the SWOT method (Strengths, Weaknesses, Opportunities, Threats) to ensure relevance to current threats. Consistent with this, research by [10] states that SWOT analysis is highly effective for identifying strengths, weaknesses, opportunities, and threats related to information security, enabling organizations to prioritize appropriate mitigation strategies. Furthermore, the use of vulnerability scanners to detect security gaps; security certifications such as ISO 27001 or HIPAA; penetration testing to identify system vulnerabilities; implementation of Web Application Firewalls (WAF) or database firewalls for layered security; deployment of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS); and data encryption using protocols such as SSL/TLS for securing communication and data storage have been proven effective in studies by [11][12][13]. Institutions implementing these measures were shown to significantly reduce security vulnerabilities. ISO 27001, in particular, is widely recognized as a global security standard that strengthens risk management and information security capabilities, in alignment with COBIT 2019 principles that prioritize the protection of health information.

In the APO12 domain (Risk Management), the implementation of an Information Security Management System (ISMS) based on the ISO 27001 standard is also required. Research by [14] demonstrates that effective ISMS implementation reduces security incident risks by providing clear guidelines for information risk management. Centralized incident reporting systems such as Security Information and Event

Management (SIEM) have been proven to support real-time threat detection, as recommended by [15]. Furthermore, the application of machine learning techniques to classify incident types can improve the speed and accuracy of response mechanisms. This approach is consistent with findings by [16], which show that machine learning algorithms integrated into SIEM systems produce accurate results in early threat detection.

In the APO13 domain (Security Management), Semen Padang Hospital needs to enhance human resource capacity through basic security training and professional security certifications. According to [17], certifications such as CISSP, CISM, and CompTIA Security+ are highly beneficial in improving staff competencies and organizational resilience against cyber threats. Such training aims to ensure that employees understand secure system usage practices, including phishing avoidance and strong password management. A study by [18] indicates that security weaknesses often originate at the end-user level, making training and awareness critical components in reducing human-error-related risks.

4. CONCLUSION

Based on the audit conducted using the COBIT 2019 framework, the Hospital Management Information System (HMIS) at Semen Padang Hospital is currently at Security Capability Level 2. The evaluation, carried out through the EDM03, APO12, and APO13 processes, identified the need for scheduled improvements and phased system development to achieve the expected standards. The implementation of the previously outlined mitigation measures is essential to ensure system security, mitigate potential risks, and achieve sustained compliance with information security standards. Although adequate progress has been achieved, continuous efforts remain necessary to enhance system performance and address potential vulnerabilities identified during the audit.

REFERENCES

[1] A. Chauhan and R. Singh, “Information Technology Role in Hospital Administration practices,” *Int. J. Manag. (IJM*, vol. 7, no. 4, pp. 108–115, [Online]. Available: http://www.iaeme.com/IJM/index.asp108http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType =7&IType=4JournalImpactFactor

[2] R. Molly and M. Itaar, “Analisis Pemanfaatan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Pada RRSUD DOK II Jayapura,” 2021. [Online]. Available: https://journal-computing.org/index.php/journal-sea/index

[3] Kemenkes RI, “Permenkes No 3 Tahun 2020 Tentang Klasifikasi dan Perizinan Rumah Sakit,” *Tentang Klasifikasi dan Perizinan Rumah Sakit*, no. 3, pp. 1–80, 2020, [Online]. Available: http://bppsdmk.kemkes.go.id/web/filesa/peraturan/119.pdf

[4] M. A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, “Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI,” vol. 4, no. 1, pp. 19–26, 2023.

[5] P. I. I. S. Listyorini, “Sistem Keamanan SIMRS di Rumah Sakit,” *Pros. Semin. Inf. Kesehat. Nas.*, pp. 234–240, 2021.

[6] Y. A. Wilar, K. Yuliawan, and A. A. Natsir, “Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire,” *MAHESA Malahayati Heal. Student J.*, vol. 3, no. 10, pp. 3365–3374, 2023, doi: 10.33024/mahesa.v3i10.11246.

[7] A. D. Yaner, H. Tanuwijaya, and E. Sutomo, “AUDIT KEAMANAN SISTEM INFORMASI PADA INSTALASI SISTEM INFORMASI MANAGEMENT (SIM-RS) BERDASARKAN STANDAR ISO 27002 (Studi Kasus: Rumah Sakit Umum Haji Surabaya) Annisa,” *J. Sist. Inf. Komput. Akunt.*, vol. 1, no. 1, pp. 1–8, 2012.

[8] ISACA, *COBIT 2019 Framework Introduction and Methodology*. 2019.

[9] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[10] R. Ayyagari, V. Grover, and R. Purvis, “Technostress: Technological antecedents and implications,” *MIS Q. Manag. Inf. Syst.*, vol. 35, no. 4, pp. 831–858, 2011, doi: 10.2307/41409963.

[11] X. Liu, J. Gao, X. He, L. Deng, K. Duh, and Y. Y. Wang, “Representation learning using multi-task deep neural networks for semantic classification and information retrieval,” *NAACL HLT 2015 - 2015 Conf. North Am. Chapter Assoc. Comput. Linguist. Hum. Lang. Technol. Proc. Conf.*, pp. 912–921, 2015, doi: 10.3115/v1/n15-1092.

[12] R. F. Chen and J. L. Hsiao, “An investigation on physicians’ acceptance of hospital information systems: A case study,” *Int. J. Med. Inform.*, vol. 81, no. 12, pp. 810–820, 2012, doi: 10.1016/j.ijmedinf.2012.05.003.

[13] W. W. Widiyanto, “SIMRS Network Security Simulation Using Snort IDS and IPS Methods,” *Indones.*

Heal. Inf. Manag. J., vol. 10, no. 1, pp. 10–17, 2022, doi: 10.47007/inohim.v10i1.396.

[14] M. E. Whitman and H. J. Mattord, “Information Security Governance for the Non-Security Business Executive,” *J. Exec. Educ.*, vol. 11, no. 1, pp. 97–111, 2012.

[15] H. Khotimah, F. Bimantoro, and R. S. Kabanga, “Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat,” *J. Begawe Teknol. Inf.*, vol. 3, no. 2, pp. 213–219, 2022, doi: 10.29303/jbegati.v3i2.752.

[16] G. Martha and G. Bororing, “Evaluasi Kinerja Algoritma Machine Learning Dalam Prediksi Serangan Malware,” *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 3060–3066, 2024.

[17] T. G. Laksana and S. Mulyani, “Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan,” *J. Ilm. Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024, doi: 10.56127/jukim.v3i01.1143.

[18] Person, “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (Mcda),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.