Risk-Based Evaluation of Hospital Management Information System Implementation Using ISO 31000 Framework

Rinno Petra Amzar
Universitas Bina Nusantara; Jakarta, Indonesia
E-mail: rinno.amzar@binus.ac.id

Nilo Legowo
Universitas Bina Nusantara; Jakarta, Indonesia
E-Mail: nlegowo@binus.edu

Submitted:
SEPTEMBER 2025

Accepted:
DECEMBER 2025

ABSTRACT

The implementation of a hospital management information system in Indonesian public hospitals brings opportunities for service improvement as well as various risks that must be carefully managed. This study evaluated the implementation of hospital management information system, using the ISO 31000:2018 risk management framework. Using a mixed methods approach, the study identified key risks in the technical, operational, human resources, and infrastructure domains through interviews, field observations, and document analysis. Each risk was analyzed for its likelihood and impact using a quantifiable risk matrix according to the ISO 31000 standard. The evaluation results indicated that system disruptions due to software and network instability, lack of training leading to user errors, and failure of data integration between modules were the most significant risks faced. Several other risks included the threat of cyberattacks on patient data, limited skilled IT personnel, and suboptimal network infrastructure capacity. Recommended mitigation strategies include continuous improvement of user training programs, investment in information technology infrastructure, implementation of stringent cybersecurity protocols, and regular system audits and monitoring. This study produces a practical risk-based evaluation model for the implementation of hospital management information system in regional hospitals, using an internationally recognized risk management framework.

Keywords*: Digital Health Transformation, Health Information Technology, Hospital Management Information System, ISO 31000, Risk Assessment, Risk Management.*

ABSTRAK

Penerapan sistem informasi manajemen rumah sakit di rumah sakit umum di Indonesia menghadirkan peluang peningkatan layanan sekaligus berbagai risiko yang harus dikelola dengan cermat. Studi ini mengevaluasi penerapan sistem informasi manajemen rumah sakit menggunakan kerangka kerja manajemen risiko ISO 31000:2018. Dengan menggunakan pendekatan metode campuran, studi ini mengidentifikasi risiko-risiko utama dalam domain teknis, operasional, sumber daya manusia, dan infrastruktur melalui wawancara, observasi lapangan, dan analisis dokumen. Setiap risiko dianalisis tingkat kemungkinan dan dampaknya menggunakan matriks risiko terukur sesuai standar ISO 31000. Hasil evaluasi menunjukkan bahwa gangguan sistem akibat ketidakstabilan perangkat lunak dan jaringan, kurangnya pelatihan yang menyebabkan kesalahan pengguna, dan kegagalan integrasi data antar modul merupakan risiko paling signifikan yang dihadapi. Beberapa risiko lainnya meliputi ancaman serangan siber terhadap data pasien, keterbatasan tenaga TI terampil, dan kapasitas infrastruktur jaringan yang belum optimal. Strategi mitigasi yang direkomendasikan meliputi peningkatan berkelanjutan program pelatihan pengguna, investasi dalam infrastruktur teknologi informasi, penerapan protokol keamanan siber yang ketat, serta audit dan pemantauan sistem secara berkala. Studi ini menghasilkan model evaluasi berbasis

JIMKES

Jurnal Ilmiah Manajemen Kesatuan
Vol. 13 No. 6, 2025
pp. 5179-5190
IBI Kesatuan
ISSN 2337 – 7860
E-ISSN 2721 – 169X
DOI: 10.37641/jimkes.v13i6.4221

risiko praktis untuk implementasi sistem informasi manajemen rumah sakit di rumah sakit regional, menggunakan kerangka kerja manajemen risiko yang diakui secara internasional.

***Keywords**: Transformasi Kesehatan Digital, Teknologi Informasi Kesehatan, Sistem Informasi Manajemen Rumah Sakit, ISO 31000, Penilaian Risiko, Manajemen Risiko, SIMRS.*

INTRODUCTION

The digitalization of health services has become a national priority in Indonesia, aligning with the government's push to implement integrated information systems in health facilities (Firdaus et al., 2025). The Ministry of Health, through regulations such as Permenkes Number 82 of 2013, mandates every hospital to adopt a Hospital Management Information System (*Sistem Informasi Manajemen Rumah Sakit*/SIMRS) to improve efficiency, service quality, and accountability (Lelyana & Sarjito, 2025). This digital transformation offers significant opportunities but also presents challenges, such as limited infrastructure and user readiness, particularly in regional hospitals (Mutiarani, 2023). SIMRS serves not only as a tool for digitizing medical records and clinical administration but also as a backbone for enhancing operational efficiency, service quality, and decision-making accuracy in hospitals (Maharani & Aisah, 2024). By integrating electronic medical records and enabling real-time data exchange between units like pharmaceuticals, laboratories, and the Social Security Administration Agency (*Badan Penyelenggara Jaminan Sosial*/BPJS) insurance claims, SIMRS accelerates service processes and reduces the potential for medical errors. The adoption of management information systems, as seen in various sectors, also supports better monitoring and decision-making, which is critical for hospital operations (Ali et al., 2025).

Mandau Hospital, a regional general hospital in Bengkalis Regency, Riau Province, has implemented SIMRS almost comprehensively. According to the 2021 Performance Report of Mandau Hospital, the level of computer system integration across various service units has reached 99%. This achievement reflects a strong commitment to digital transformation. However, the success of SIMRS implementation is not without challenges. The hospital's management still faces operational and technical risks, including limited user training, system disruptions, and suboptimal supporting infrastructure. These challenges highlight the need for structured risk management to ensure the system's sustainability and effectiveness (Setiawan & Wijayati, 2024).

Common technical risks include network outages, system instability that hinders real-time data integration, hardware failures, and cybersecurity threats like malware attacks on patient data. Non-technical risks, such as operational and human resource issues, include human errors in system use (e.g., incorrect data entry) due to insufficient training, a shortage of skilled IT personnel, and potential misalignment of SIMRS with established operational standards (Cita et al., 2025; Gunawan, 2024). If not managed properly, these risks can reduce the hospital's operational effectiveness and hinder the goal of improving health service quality. Previous studies, such as those by Hutagalung (2022), have explored risk management in SIMRS but often focused on large urban hospitals, leaving a gap in understanding the specific challenges faced by regional hospitals with limited resources. Many hospitals struggle with technical and human resource risks, yet there is little research on applying international risk management standards like ISO 31000 in smaller, regional contexts. This research gap underscores the need to evaluate SIMRS implementation in regional hospitals using a globally recognized framework to address their unique constraints.

For this reason, implementing an international standard for risk management is crucial for SIMRS governance. ISO 31000:2018, a globally recognized and adaptable risk management framework, is well-suited for the healthcare sector (Hutagalung, 2022; Putra & Hendrawan, 2024). This framework was chosen because it provides a flexible, systematic approach to identifying, analyzing, and mitigating risks, which is essential for managing the complex challenges of SIMRS in resource-constrained settings. It

emphasizes a continuous process of identifying risk sources, analyzing their likelihood and impact, evaluating risk acceptability, and applying appropriate mitigation strategies (Lutvi et al., 2024). Additionally, integrating the DeLone and McLean (2003) Information Systems Success Model allows this study to assess not only risk mitigation but also the overall success of SIMRS in terms of system quality, user satisfaction, and organizational benefits.

This research aims to apply the ISO 31000 framework to evaluate SIMRS implementation at Mandau Hospital. The specific objectives are to: (1) identify the types of risks arising during SIMRS implementation, (2) analyze the causes and domains (technical, operational, human resources, infrastructure) of these risks, (3) assess the likelihood and impact of each risk using a risk matrix, and (4) formulate mitigation strategies to minimize critical risks. The study seeks to fill the research gap by providing a risk-based evaluation model tailored for regional hospitals, using an internationally recognized framework. The results are expected to contribute to the risk management literature in the healthcare sector and offer practical recommendations for Mandau Hospital and similar institutions to enhance the success and sustainability of their SIMRS.

LITERATURE REVIEW

Hospital Management Information System

A Hospital Management Information System (*Sistem Informasi Manajemen Rumah Sakit*/SIMRS) is an integrated system designed to manage all aspects of hospital operations, including administrative, clinical, and managerial processes. According to Windarti and Nadya (2023) and Diaz (2025), SIMRS connects various functional modules, such as patient registration, medical records, pharmacy, laboratory, radiology, and finance, into a single digital platform. This integration ensures smooth data flow between units, reducing duplication and improving service accuracy and efficiency. For instance, data entered in the registration unit is instantly available to clinics, pharmacies, and billing, which shortens wait times and minimizes errors from repeated entries. As shown in Figure 1, the integrated SIMRS architecture illustrates how various modules connect to a central database, enabling real-time data exchange across hospital units.

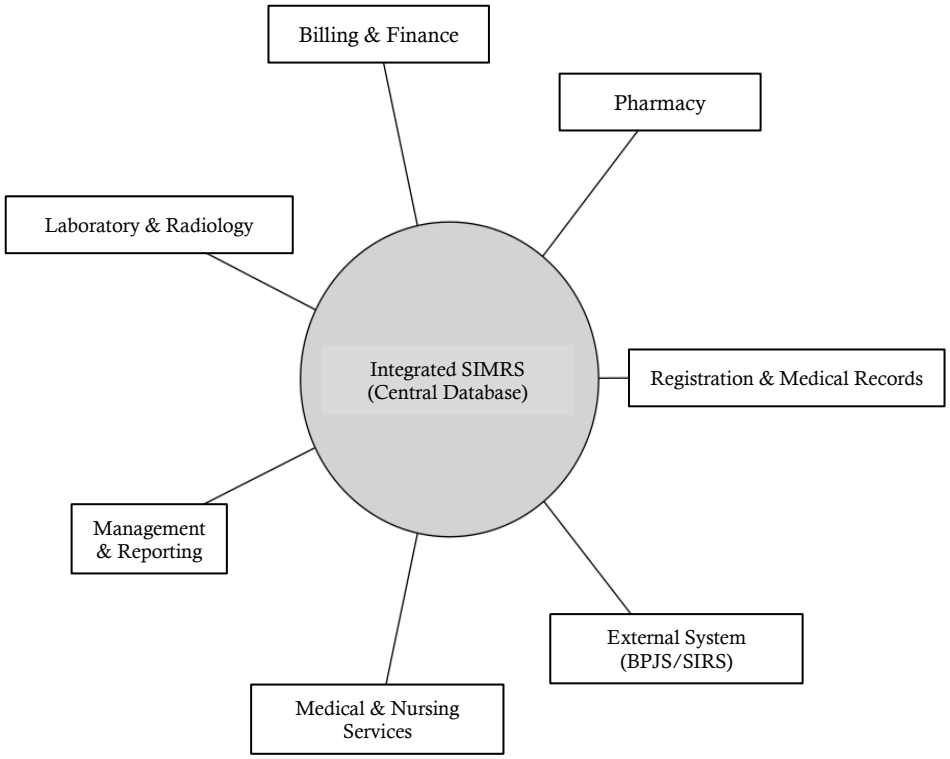

Figure 1. Illustration of the Integrated SIMRS Architecture

The benefits of SIMRS are well-documented in various studies. Supriyadi et al. (2025) note that SIMRS improves operational efficiency, speeds up service workflows, and reduces manual administrative tasks. It also enhances patient data processing, increases recording accuracy, and supports better clinical services. Additionally, SIMRS contributes to long-term cost savings by reducing paper use, optimizing drug inventory, and streamlining billing systems to minimize uncollectible receivables. In line with Indonesia's One Health Data program, SIMRS must comply with regulations like Permenkes Number 82 of 2013, ensuring interoperability with government systems such as SIRS and BPJS (Windarti & Nadya, 2023). However, Nor et al. (2024) highlight that operational challenges, such as inconsistent data entry and system adaptation, can hinder SIMRS effectiveness, particularly in hospitals with limited resources. This emphasizes the need for robust change management to maximize SIMRS benefits.

Despite its advantages, SIMRS implementation faces significant challenges, especially in regional hospitals. Technical issues, such as system compatibility, downtime due to network or power outages, software bugs, and cybersecurity threats like malware, are common obstacles (Fathurohman et al., 2025). Human resource challenges, including user resistance and insufficient training, often lead to underutilization of the system (Matimbwa & Masue, 2019; Nyawira et al., 2022; Hidayatuloh et al., 2025). According to Jasmine et al. (2025), undisciplined use of SIMRS modules can create bottlenecks in service workflows, underscoring the need for comprehensive risk management to address both technical and non-technical issues. These challenges highlight the importance of a structured approach to ensure SIMRS achieves its intended outcomes.

ISO 31000:2018 Risk Management Framework

ISO 31000:2018 is an international standard offering general guidance for risk management across various sectors, including healthcare (Ginting, 2024). According to Putra and Hendrawan (2024), this framework emphasizes integrating risk management into organizational governance through a continuous cycle of context setting, risk assessment, and treatment. It is flexible and adaptable, making it suitable for managing complex risks in hospital settings. As illustrated in Figure 2, the ISO 31000 process starts with establishing the risk context, followed by identification, analysis, and evaluation of risks, with ongoing communication, consultation, and monitoring throughout. The framework's principles include stakeholder involvement, customization to context, and the use of the best available information.

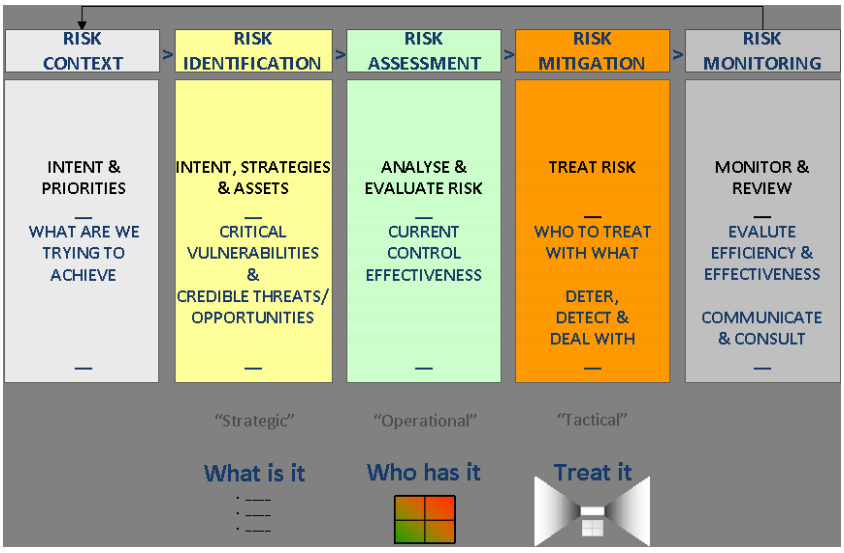

Figure 2. Flow Diagram of the Risk Management Process based on ISO 31000:2018

The risk management process in ISO 31000 involves identifying risks, analyzing their likelihood and impact, and evaluating their acceptability. Hubbard (2020) explains that tools like risk matrices help organizations assess risk severity by combining likelihood and consequence scores. In the context of SIMRS, risks can include technical issues like system failures, operational disruptions, human errors, and infrastructure limitations. Björnsdottir et al. (2022) argue that ISO 31000 is effective in identifying hidden organizational risks, making it valuable for hospitals managing sensitive patient data. Regular monitoring and review ensure that new risks are captured and mitigation strategies remain effective (Permatasari, 2025). However, Efe (2023) and Nasution et al. (2025) note that while ISO 31000 is widely applicable, frameworks like NIST or COSO may offer more specific guidance for cybersecurity risks, suggesting a need to compare their applicability in SIMRS contexts.

Despite its strengths, ISO 31000 has limitations in resource-constrained settings like regional hospitals. According to Ispas et al. (2023), implementing integrated management systems based on ISO 31000 requires significant resources and expertise, which may be challenging for smaller hospitals. Selvaseelan (2018) suggests that supplementary frameworks, such as the Risk-Sentience Auxiliary Framework (RSAF), can enhance ISO 31000 in high-risk environments like healthcare. Additionally, Basri and Ayu (2024) demonstrate that combining ISO 31000 with ISO/IEC 27001 can strengthen cybersecurity risk management in health information systems, addressing a critical gap in SIMRS implementation. These insights highlight the need for tailored risk management strategies to ensure SIMRS success in regional hospitals.

DeLone & McLean Information Systems Success Model

The DeLone and McLean information systems success model provides a framework to evaluate the success of information systems like SIMRS. According to Alshehri and Hadoussa (2025), this model measures success through six dimensions: system quality, information quality, service quality, use/intention to use, user satisfaction, and net benefits. System quality focuses on technical performance, such as reliability and ease of use, which are critical for SIMRS stability and integration with devices like BPJS portals. Information quality ensures that SIMRS outputs, such as medical or management reports, are accurate and timely for decision-making. Service quality reflects the responsiveness of IT support, which is vital for addressing user issues.

The DeLone and McLean (2003) model highlights the interdependence of its dimensions. Kartini et al. (2025) note that high system and information quality drive increased system use and user satisfaction, leading to greater organizational benefits. For SIMRS, these benefits include improved staff productivity, cost savings, and enhanced patient services. Afifawati et al. (2023) and Farhan et al. (2025) emphasize that disruptions, such as system downtime or human errors, can undermine these dimensions, particularly in environments with multiple risks. By addressing risks identified through ISO 31000, hospitals can enhance system quality and user satisfaction, ensuring SIMRS delivers its intended benefits. This study integrates the DeLone and McLean model with ISO 31000 to evaluate both the protective (risk mitigation) and promotive (system success) aspects of SIMRS implementation, offering a comprehensive approach to assessing its effectiveness.

RESEARCH METHODS

This study employed a qualitative method to thoroughly understand the risks associated with the implementation of SIMRS at Mandau Hospital. The research process began with a preliminary study to establish the risk context, followed by data collection for risk identification, risk analysis, and evaluation using a risk matrix, and the formulation of mitigation recommendations. Initial activities included document reviews and field observations to understand the SIMRS environment, system structure, and documented issues. The 2021 Mandau Hospital performance report provided secondary data on SIMRS implementation achievements and performance indicators.

Data collection involved in-depth interviews with key stakeholders, such as the head of the hospital's IT department, SIMRS administrators, and user representatives from various units. These interviews explored user experiences, challenges, and perceived risks in daily SIMRS operations. Additionally, a structured questionnaire was distributed to assess system outages, downtime duration, user satisfaction, and infrastructure readiness. The collected data were compiled into a risk register, listing identified risks along with their sources, potential impacts, and categories (technical, operational, human resources, or infrastructure). Examples include system downtime during peak hours, user errors in data entry, and network disconnections due to outdated equipment.

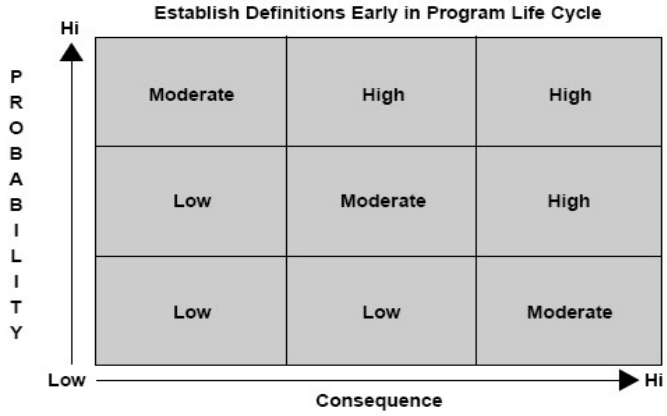

Figure 3. Risk Assessment Matrix

For risk analysis, each identified risk was evaluated based on its likelihood and impact using a 5x5 risk matrix, as shown in Figure 3. The likelihood was rated from 1 (rare) to 5 (almost certain), and the impact was rated from 1 (negligible) to 5 (critical), based on hospital operational data and stakeholder input. Risk scores were calculated by multiplying these ratings, with scores of 1–6 classified as low (green), 7–14 as moderate (yellow), and 15 or higher as high (red). To address potential bias, such as overreporting of issues by users, the research team cross-verified questionnaire responses with IT department logs and conducted Focus Group Discussions (FGDs) with hospital management to validate findings. This matrix, depicted in Figure 3, helped visualize the risk profile and prioritize mitigation efforts.

Risk evaluation focused on high and moderate risks, determining whether they were adequately managed or required further action. FGDs with hospital management ensured the feasibility of proposed mitigation strategies. Recommendations were developed using a Specific, Measurable, Achievable, Relevant, Time-bound (SMART) approach, prioritizing risks impacting patient safety and service continuity. These included technical solutions like server upgrades, procedural changes like IT incident response protocols, and human resource enhancements like regular training, each assigned to responsible parties with short- or long-term timelines. This structured approach ensured that the study provided practical and actionable insights for Mandau Hospital to enhance SIMRS implementation.

RESULTS

Overview of Identified Risks in SIMRS Implementation

This study systematically evaluated the risks associated with the implementation of SIMRS at Mandau Hospital, using the ISO 31000 framework to identify, analyze, and prioritize potential challenges. By combining qualitative and quantitative methods, the research mapped a comprehensive risk profile, revealing critical vulnerabilities in the hospital's digital transformation efforts. The findings provide actionable insights for improving SIMRS implementation, particularly in regional hospitals with limited

resources. As illustrated in Figure 4, the distribution of risks across technical, operational, human resources, and infrastructure domains highlights the complexity of managing a health information system in such settings.

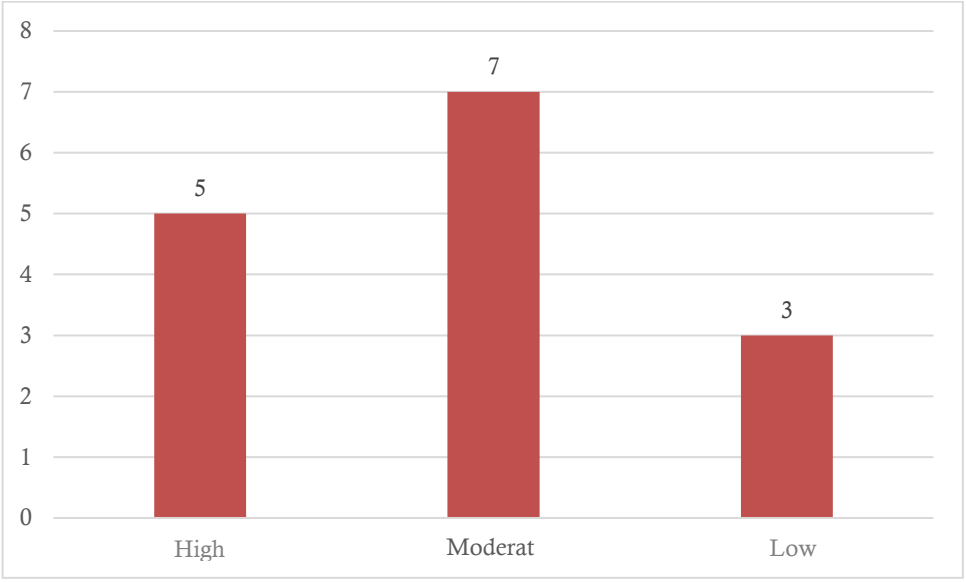

Figure 4. Graph of Amount and Risk Level

The evaluation identified a total of fifteen risks related to SIMRS implementation at Mandau Hospital, categorized into four main domains: technical, operational, human resources, and infrastructure. These risks were assessed for their likelihood and impact, resulting in a distribution of five high-level risks, seven moderate risks, and three low risks. As depicted in Figure 4, a bar chart summarizes the number of risks in each domain and their severity, showing that technical and human resource risks dominate the high-risk category. Technical risks, such as system downtime and data integration failures, were found to be particularly critical due to their direct impact on patient services. Human resource risks, driven by inadequate training, also posed significant challenges. Operational and infrastructure risks, while fewer in number, still required attention to ensure system reliability. This distribution, detailed in Table 1, underscores the need for targeted mitigation strategies to address the most pressing risks first.

Table 1. Risk Levels Per Category

Category	Details	Level Risk
Technical	System Downtime and Instability	Tall
	Data Integration Failure	Tall
	Cybersecurity Threats	Tall
	Hardware Breakdown	Moderate
	Software Feature Incompatibilities	Moderate
Operational	Service Process Disrupted Due to Not Optimal Adaptation	Moderate
	Dependency on the System	Moderate
	Process Compliance and Standardization	Low
TBSP	Lack of User Training and Competence	Tall
	Internal IT Workforce Limitations	Tall
	User Resistance or Motivation	Moderate
	Human Error	Moderate
Infrastructure	Network and Hardware Limitations	Moderate
	Electrical Power Supply Disruption	Low
	Disaster or Physical Damage	Low

Technical risks emerged as a major concern, encompassing issues related to software, hardware, networking, and information system security. System downtime, caused by

software bugs or server crashes, was a prominent issue. For instance, a thirty-minute downtime during morning registration hours led to patient queues and manual recording errors, disrupting service flow. This risk was rated high due to its frequent occurrence during peak hours and its significant impact on registration and medical record access. The severity of this risk, as shown in Table 1, reflects its score of 16 (likelihood 4, impact 4) on the risk matrix. Data integration failures, where laboratory results appeared late in the doctor's module due to slow database replication, were another critical issue. This risk, rated with a likelihood of 3 and an impact of 5, could jeopardize clinical decisions, particularly in emergencies. Cybersecurity threats, such as a malware attack that infected client computers, were also notable. Although the attack did not spread to the server, the risk was rated moderate to high due to increasing global cyber threats. Other technical risks included hardware damage, such as disk crashes, and software incompatibilities requiring manual workarounds, both rated as moderate but necessitating a business continuity plan.

Analysis of Risks Across Domains

Operational risks related to hospital business processes and adaptation to SIMRS were generally less severe but still impactful. Some service units experienced slowdowns during the transition from manual to electronic procedures. For example, the pharmaceutical department faced delays because prescriptions had to be entered into SIMRS before dispensing, causing longer patient queues initially. This risk was rated moderate, as process adjustments have reduced its frequency over time. High system dependency also posed a challenge, when SIMRS failed, nearly all processes, from card printing to billing, were disrupted, highlighting the need for manual backup procedures. Non-compliance with data entry standards, such as delayed drug order entries by doctors, led to pharmacy delays and stock mismatches. Operational risks are fewer but still contribute to service inefficiencies, as seen in their moderate risk classification. Continuous evaluation and standard operating procedure adjustments have helped mitigate these issues, but proactive change management remains essential.

Human resource risks were among the most significant, driven by user-related challenges. Insufficient training led to frequent data entry errors, such as duplicate patient records or incorrect drug dosages, with a high risk score due to their clinical and financial implications. For example, a front office officer created duplicate patient data by misunderstanding the system's search function, while a nurse entered an incorrect dosage due to misreading the interface. This risk has a score of 12 (likelihood 4, impact 3), placing it in the high-risk zone. The limited number of IT personnel, with only three staff members managing all hospital IT needs, created vulnerabilities when the team was overwhelmed or absent. This risk, rated moderate, underscored a knowledge gap, as the hospital often relied on vendors for complex issues. Some senior staff resisted SIMRS, preferring manual methods, which affected data quality. These human resource risks fall in the red and yellow zones, indicating their priority for mitigation. Appointing super-users in each unit and conducting regular training every six months have been short-term solutions, but ongoing capacity building is critical.

Infrastructure risks, related to physical IT support like networks, electricity, and hardware, were generally low to moderate. Weak Wi-Fi signals in areas like the radiology room slowed SIMRS access, while outdated client PCs hindered performance. This risk is moderate, with a score of 8 (likelihood 2, impact 4), due to its impact on specific units. Power outages, despite the presence of a generator, caused brief server disruptions because the transition to backup power took about one minute. This risk, rated low to moderate, still required attention to ensure uninterrupted healthcare services. Natural disasters, such as flooding, posed a rare but potential threat to equipment, mitigated by off-site backups and secure server placement. Infrastructure risks are less frequent but foundational to SIMRS reliability. Gradual hardware upgrades, increased bandwidth, and regular maintenance were recommended to strengthen infrastructure.

The risk evaluation process prioritized high and moderate risks for immediate action. System downtime, lack of user training, and data integration failures were identified as top priorities due to their severe impact on patient safety and service continuity. Cybersecurity threats and limited IT personnel, while slightly lower in score, were also flagged for urgent mitigation given rising external threats. Low-level risks, such as minor resistance or brief power outages, were deemed acceptable with routine monitoring. This prioritization aligns with the hospital's low risk tolerance for disruptions to essential services. Focus group discussions with management validated these findings and ensured that proposed mitigations, such as server upgrades, enhanced training, and cybersecurity protocols, were feasible and aligned with hospital goals.

DISCUSSION

This study reveals that the implementation of the SIMRS at Mandau Hospital has achieved a high adoption rate, with 99% unit integration, yet it faces significant risks across technical, operational, human resources, and infrastructure domains. A total of fifteen risks were identified, with five classified as high, seven as moderate, and three as low, confirming the complexity of digital transformation in healthcare. According to Jasmine et al. (2025), technical and human resource risks, such as system downtime and user errors, are common challenges in SIMRS implementation, particularly in regional hospitals. These findings align with prior research, which highlights that system stability and user competence are critical for successful digitalization (Putri et al., 2025). The high-risk profile at Mandau Hospital, as shown by Setiawan and Wijayati (2024), mirrors challenges in other regional hospitals where limited resources amplify technical and human vulnerabilities.

Technical risks, including system downtime and data integration failures, significantly disrupt patient services. Downtime during peak hours, for instance, delays registration and medical record access, increasing wait times and risking manual errors. Similarly, integration failures delay critical data like laboratory results, potentially affecting clinical decisions. These issues resonate with findings by Hidayat et al. (2022), who note that system outages in health information systems directly reduce service quality. Basri and Ayu (2024) emphasize that cybersecurity risks, another key concern at Mandau Hospital, require robust measures like firewalls and user training to protect sensitive patient data. The study's use of the ISO 31000 framework effectively mapped these risks, enabling prioritization of mitigation strategies that address immediate threats to service continuity.

Human resource risks, particularly inadequate training and limited IT staff, are equally critical. Frequent user errors, such as incorrect data entries, compromise medical and financial accuracy, echoing Sinulingga et al. (2025), who stress that user competence is a key determinant of system success. The small IT team at Mandau Hospital struggles to manage system demands, often relying on vendors, which creates delays in issue resolution. Ispas et al. (2023) argue that resource-constrained settings, like regional hospitals, face challenges in implementing comprehensive risk management due to limited expertise, underscoring the need for ongoing training and capacity building. Mandau Hospital's approach of appointing super-users and conducting regular training is a step forward, but sustained investment in human resources is essential to reduce errors and enhance system utilization.

Operational risks, such as system dependency and non-compliance with data entry standards, highlight the need for better change management. High reliance on SIMRS, while a sign of successful adoption, leaves services vulnerable during outages, necessitating manual backup procedures. Non-compliance, like delayed drug order entries, causes workflow inefficiencies, as noted by Famila et al. (2025). Suarmanayasa et al. (2024) suggest that adopting SMART strategies can improve procedural compliance, a principle applied in this study's mitigation recommendations. These findings emphasize the importance of aligning SIMRS processes with hospital workflows to maintain service efficiency.

Infrastructure risks, though less severe, impact system reliability. Weak Wi-Fi signals and outdated hardware slow data access, while power outages disrupt operations. Febriana et al. (2025) highlight that gradual infrastructure investments significantly enhance system sustainability. Riyadi and Ratnasari (2025) note that prioritizing risks with high impact, like those affecting service continuity, is critical for resource allocation in constrained settings. The ISO 31000 framework's risk matrix helped Mandau Hospital prioritize high-impact risks, aligning mitigation with its low risk tolerance for patient safety disruptions.

The study's limitations include its focus on a single regional hospital, which may limit generalizability to larger or private hospitals with different resource levels. According to Setiawan and Wijayati (2024), contextual factors like budget constraints and staff readiness vary significantly across hospital types, affecting risk profiles. Budget limitations may also hinder the implementation of recommended mitigations, such as infrastructure upgrades. This study contributes to the literature by offering a tailored risk evaluation model for regional hospitals, addressing a gap noted by Ispas et al. (2023) in applying ISO 31000 to smaller healthcare settings. Integrating ISO 31000 with the DeLone and McLean model further ensures that risk mitigation supports system quality and user satisfaction, enhancing SIMRS success.

CONCLUSION

This study confirms that Mandau Hospital has successfully implemented the SIMRS with a 99% integration rate across service units, demonstrating a strong commitment to digital transformation. However, the evaluation using the ISO 31000 framework revealed fifteen risks across technical, operational, human resources, and infrastructure domains, with system downtime, inadequate user training, and data integration failures identified as the most critical. These risks, if not addressed, can undermine service quality and patient safety. By applying a 5x5 risk matrix, the study prioritized high-impact risks and proposed actionable mitigation strategies, such as server upgrades, regular training, and enhanced cybersecurity measures, to strengthen SIMRS reliability. The integration of ISO 31000 with the DeLone and McLean model provided a comprehensive approach, ensuring that risk management supports system quality, user satisfaction, and organizational benefits.

The findings offer practical implications for regional hospitals, providing a structured model to manage SIMRS risks and enhance operational efficiency. However, the study's focus on a single regional hospital limits its generalizability to larger or private hospitals with different resources. Budget constraints may also challenge the implementation of recommended mitigations, such as infrastructure upgrades. For future research, exploring SIMRS risks in diverse hospital settings, such as urban or private facilities, could validate the model's applicability. Additionally, investigating the role of emerging technologies, like artificial intelligence or cloud computing, in mitigating SIMRS risks could further enhance system sustainability and performance.

REFERENCES

[1] Afifawati, N., Khasanah, L., & Giovanni, A. (2023). Interplay of risk management in the multi-disruption era and agency theory insights: A literature review. *Jurnal Ilmiah Manajemen Kesatuan, 11*(2), 505–512.

[2] Ali, H., Sirat, A. H., & Nurhaida, I. (2025). Implementation of management information systems in monitoring creative economic development. *Jurnal Ilmiah Manajemen Kesatuan, 13*(1), 233–246.

[3] Alshehri, A., & Hadoussa, S. (2025). Reevaluating the DeLone and McLean model for EHR success and knowledge-sharing in a Saudi public medical complex. *Journal of Information Technology Management, 17*(2), 28–49.

[4] Basri, W. S., & Ayu, A. L. (2024). Risk management in information systems: Applying ISO 31000: 2018 and ISO/IEC 27001: 2022 controls at PMI's central clinic. *International Journal for Applied Information Management, 4*(1), 1–13.

[5] Björnsdottir, S. H., Jensson, P., Thorsteinsson, S. E., Dokas, I. M., & de Boer, R. J. (2022). Benchmarking ISO risk management systems to assess efficacy and help identify hidden organizational risk. *Sustainability, 14*(9), 4937–4950.

[6] Cita, Y., Miranda, A., Fandani, M., Mahputra, S., Irawan, I. A. F., & Paramarta, V. (2025). Tantangan implementasi SIMRS dari perspektif tenaga kesehatan: Studi kualitatif di rumah sakit daerah [Challenges of SIMRS implementation from the perspective of health personnel: A qualitative study in a regional hospital]. *Al-Ihtiram: Multidisciplinary Journal of Counseling and Social Research, 4*(1), 121–132.

[7] DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9–30.

[8] Diaz, A. S. (2025). The influence of the implementation of the hospital management information system (SIMRS) on the effectiveness of patient administration services at Grandmed Hospital Lubuk Pakam. *MEDISTRA Medical Journal, 2*(2), 72–76.

[9] Efe, A. (2023). A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Denetim ve Güvence Hizmetleri Dergisi, 3*(2), 185–205.

[10] Famila, F., Yudha, G. A. K., Bambulu, G., & Veranita, M. (2025). Transformasi manajemen rumah sakit di era digital: Tinjauan literatur dalam fokus pengembangan sumber daya manusia. *Blantika: Multidisciplinary Journal, 3*(8), 1120–1132.

[11] Farhan, F. G. R., Indriati, R., & Harini, D. (2025). Evaluasi persepsi pengguna sistem informasi manajemen rumah sakit (SIMRS) pada rawat jalan. *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi), 9*(2), 961–968.

[12] Fathurohman, A., Setiawan, R., & Darmawan, F. E. (2025). Analisis risiko jaringan komputer untuk meningkatkan kualitas keamanan pada jaringan komputer rumah sakit Universitas Muhammadiyah Semarang. *Proceeding of Informatics Collaborations and Dissemination Meeting, 1*(1), 45–52.

[13] Febriana, A. A., Wijaya, A., & Budiman, J. A. (2025). Peran komputasi awan dalam meningkatkan efisiensi infrastruktur teknologi informasi di sektor publik. *Network: Jurnal Teknologi Informasi, Komunikasi dan Komputer Sains, 1*(1), 11–19.

[14] Firdaus, R., Syeira, K., & Wijaya, N. (2025). Transformasi digital sistem informasi kesehatan menuju layanan kesehatan yang terkoneksi dan berpusat pada pasien. *Economics and Digital Business Review, 6*(2), 1045–1055.

[15] Ginting, R. A. H. (2024). *Enterprise risk management (ERM) berbasis ISO 31000 pada risiko operasional rumah sakit: Studi kasus RSUP dr. Wahidin Sudirohusodo Makassar.* Makassar: Universitas Hasanuddin.

[16] Gunawan, R. (2024). Efektivitas SIMRS pada INA-CBGS terhadap ketepatan tarif klaim BPJS rawat inap di RSUD X. *Journal of Health Analysis Student, 1*(2), 67–81.

[17] Hidayat, H. M., Ramdany, R., & Samukri, S. (2022). Analisis faktor-faktor yang mempengaruhi penyerapan anggaran (studi kasus pada lingkungan Kantor Wilayah DJKN DKI Jakarta). *Jurnal Akuntansi, 11*(1), 51–63.

[18] Hidayatuloh, C., Sedarmayanti, S., & Utoyo, W. (2025). Analisis sistem informasi manajemen rumah sakit (SIMRS) terhadap peningkatan layanan kesehatan dalam mendukung implementasi rekam medis elektronik di era digital. *Innovative: Journal of Social Science Research, 5*(4), 11285–11303.

[19] Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*. Hoboken, NJ: John Wiley & Sons.

[20] Hutagalung, L. E. (2022). Analisa manajemen risiko sistem informasi manajemen rumah sakit (SIMRS) pada Rumah Sakit XYZ menggunakan ISO 31000. *Teika, 12*(1), 23–33.

[21] Ispas, L., Mironeasa, C., & Silvestri, A. (2023). Risk-based approach in the implementation of integrated management systems: A systematic literature review. *Sustainability, 15*(13), 10251–10265.

[22] Jasmine, S. T., Matondang, T. S., Pratama, M. R., & Hajijah, S. (2025). Tren, tantangan, dan solusi sistem informasi manajemen rumah sakit di Jakarta. *Surya Medika: Jurnal Ilmiah Ilmu Keperawatan dan Ilmu Kesehatan Masyarakat, 20*(1), 62–70.

[23] Kartini, A. M., Fadli, S., & Fahmi, H. (2025). The DeLone and McLean model for measuring success hospital management information system case study: Praya Regional Hospital. *JISA (Jurnal Informatika dan Sains), 8*(1), 66–73.

[24] Lelyana, N., & Sarjito, A. (2025). Application of an information system for inpatient nutrition management: An implementation study based on the Indonesian Minister of Health Regulation No. 26/2013. *AcTion: Aceh Nutrition Journal, 10*(2), 442–450.

[25] Lutvi, R., Rachmadhani, M. M., Tosofu, A. Z., Mbisikmbo, M., & Supriatna, I. I. (2024). Analisa risiko menggunakan metode likelihood dan consequence risk matriks. *Industrial Engineering Journal–System, 2*(2), 67–77.

[26] Maharani, L., & Aisah, S. (2024). Peran sistem informasi manajemen dalam meningkatkan efisiensi rumah sakit. *Jurnal Sistem Informasi, Akuntansi dan Manajemen, 4*(2), 274–283.

[27] Matimbwa, H., & Masue, O. S. (2019). Usage and challenges of human resources information system in the Tanzanian public organizations. *Journal of Human Resource Management, 7*(4), 131–137.

[28] Mutiarani, R. A. (2023). Digitalisasi pelayanan kesehatan di Indonesia: Peluang dan tantangan. *ResearchGate, 1*(1), 1–9.

[29] Nasution, T. A., Indradewa, R., Rahmat Syah, T. Y., & Pamungkas, R. A. (2025). Sistem manajemen risiko berbasis ISO 31000: 2018 di RS Khusus Tumbuh Kembang GSH. *Cerdika: Jurnal Ilmiah Indonesia, 5*(5), 1–10.

[30] Nor, S. R., Indah, D. P., & Heniwati, E. (2024). Internal control analysis of asset management system at Hospital of Tanjungpura University. *Jurnal Ilmiah Manajemen Kesatuan, 12*(6), 2141–2148.

[31] Nyawira, L., Tsofa, B., Musiega, A., Munywoki, J., Njuguna, R. G., Hanson, K., ... & Barasa, E. (2022). Management of human resources for health: Implications for health systems efficiency in Kenya. *BMC Health Services Research, 22*(1), 1046–1057.

[32] Permatasari, D. F. (2025). Evaluasi manajemen risiko berdasarkan ISO 31000: 2018 dalam proyek di PT XYZ. *Jurnal Locus Penelitian dan Pengabdian, 4*(6), 1–10.

[33] Putra, I. P. A. S., & Hendrawan, I. K. R. (2024). Analisis manajemen risiko SIMRS pada Rumah Sakit Ganesha menggunakan ISO 31000. *Jurnal Teknologi dan Informasi, 14*(1), 88–98.

[34] Putri, D. N., Purba, S. H., Layana, K., & Lubis, K. (2025). Tantangan dan solusi dalam implementasi SIMRS di rumah sakit pemerintah di Indonesia. *Jurnal Riset Ilmu Kesehatan Umum dan Farmasi, 3*(1), 13–22.

[35] Riyadi, A., & Ratnasari, V. (2025). Risk assessment and mitigation in workplace safety at energy distribution company PT XYZ. *Jurnal Ilmiah Manajemen Kesatuan, 13*(1), 209–220.

[36] Selvaseelan, J. (2018). Development and introduction of the risk-sentience auxiliary framework (RSAF) as an enabler to the ISO 31000 and ISO 31010 for high-risk environments. *Administrative Sciences, 8*(2), 22–35.

[37] Setiawan, T., & Wijayati, N. (2024). Evaluation of risk management for optimizing service quality in XYZ regional general hospital. *International Journal of Financial, Accounting, and Management, 6*(2), 301–312.

[38] Sinulingga, N. E., Kep, M., & Kep, S. (2025). *Manajemen rumah sakit*. Jakarta: Gita Lentera.

[39] Suarmanayasa, I. N., Pramesworo, I. S., Masela, A., Sucipto, B., & Launtu, A. (2024). Risk management strategies in the financial industry: Theoretical review and practical implications. *Jurnal Ilmiah Manajemen Kesatuan, 12*(4), 995–1004.

[40] Supriyadi, F., Eliandi, S., & Absharina, E. D. (2025). Literatur singkat: Efisiensi dalam sistem informasi manajemen rumah sakit. *Jurnal Cakrawala Akademika, 2*(1), 924–942.

[41] Windarti, S., & Nadya, A. (2023). *Implementasi sistem informasi manajemen rumah sakit (SIMRS)*. Yogyakarta: Penerbit NEM.