Journal of Computer Science

Research Article

Risk Assessment of Healthcare Information Systems in Indonesian Regional Government Hospitals Using ISO 27001:2022

Deo Alif Alfitrah and Nilo Leegowo

Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University, Jakarta 11480, Indonesia

Article history
Received: 02-06-2025
Revised: 20-10-2025
Accepted: 20-01-2026

Corresponding Author:
Deo Alif Alfitrah
Information Systems Management Department, BINUS Graduate Program, Master of Information Systems Management, Bina Nusantara University, Jakarta 11480, Indonesia
Email: deo.alfitrah@binus.ac.id

Abstract: The growing number of cyber-attacks targeting the healthcare sector, particularly Indonesian regional government hospitals, reflects the absence of a structured information security management system. Issues such as shared account usage, lack of staff security training, and undocumented incident reporting present serious risks to patient data. This study aims to assess the current state of information security in a government hospital using the ISO/IEC 27001:2022 standard and to propose mitigation measures based on Annex A controls. The assessment was conducted using the ISO 27001 framework and methodology. A qualitative case study approach was adopted, with data collected through semi-structured interviews, direct observations, and document analysis. The evaluation followed the Plan Do Check Act (PDCA) cycle and ISO 27005 risk assessment matrix, scoring each risk based on likelihood and impact. The results show that out of eight identified risk categories, four were classified as high namely, access management, information security policy, security awareness training, and system backup management while the rest were categorized as medium. A gap analysis indicated that many of these risks were not supported by effective controls. Recommendations include policy updates, regular training, formalized incident reporting, and annual security audits. These findings highlight the urgent need for systematic ISMS implementation to improve cybersecurity resilience and safeguard patient information in public healthcare institutions.

Keywords: Information Security, Risk Assessment, Regional Government Hospital, Healthcare IS, ISO/IEC 27001

Introduction

Healthcare systems play a pivotal role in safeguarding public health, and in the era of digital transformation, the integration of Information Technology (IT) has become instrumental in enhancing service quality and operational efficiency. According to Shipu (2023), the adoption of IT in the healthcare sector significantly improves patient outcomes and streamlines healthcare delivery. This aligns with Indonesia's Law No. 17 of 2023, which underscores the urgency of establishing an efficient Health Information System to support the nation's health objectives (Undang-Undang Republik Indonesia, 2023).

However, the rapid digitalization of healthcare also introduces critical cybersecurity challenges. As mandated by the Indonesian Ministry of Health Regulation No. 82 of 2013 on Hospital Information Management Systems, it is imperative for hospitals to uphold robust information security measures (Permenkes, 2025). The increasing complexity and connectivity of healthcare systems have rendered them vulnerable to cyber threats (Fig. 1).

Furthermore, data from the National Cyber and Crypto Agency (BSSN) indicates a concerning historical trend, as shown in Figure 2. Indonesia faced 888 million cyberattacks in 2021, and although this number dropped to 279.84 million in 2023, the frequency and scale of these attacks still pose a serious risk, particularly to critical sectors like healthcare.

Figure 3 highlights the distribution of ransomware attacks across industry sectors, with the healthcare and social assistance sector accounting for 5.42% of the total incidents.

Fig. 1: Monthly Cyberattack Traffic Anomalies in Indonesia (2023)

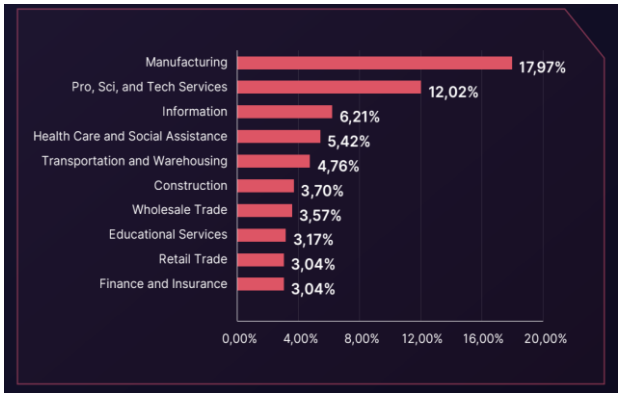

Fig. 2: Historical Trend of Cyberattacks in Indonesia (2019–2023)

Fig. 3: Distribution of Ransomware Attacks by Industry Sector

Despite not being the most targeted sector, the critical nature of healthcare data makes these attacks particularly damaging. The digitization of patient records and healthcare services has escalated the risk of data breaches and operational disruptions (Shipu, 2023).

A recent internal phishing simulation among hospital employees revealed alarming findings: 71% of users opened phishing emails, 71% clicked malicious links, and 53% entered sensitive information, while only 5% reported the incident (Nugroho and Legowo, 2022). These statistics highlight the urgent need for enhanced human-centric security measures such as training, simulated attacks, and automatic threat reporting systems.

Operationally, interviews with Indonesian Regional Government Hospitals uncovered a major incident caused by an IP address conflict between development and production servers, leading to service downtime. This event exposed deficiencies in network configuration and asset management, further emphasizing the need for structured risk management protocols.

Currently, these hospitals lack formal risk assessments and have yet to implement a comprehensive Information Security Management System (ISMS). To mitigate escalating threats, a proactive approach is required starting with systematic risk identification, evaluation of vulnerabilities, and prioritization of controls based on criticality.

ISO/IEC 27001 serves as a globally recognized framework for establishing, implementing, and continuously improving ISMS. Its application in healthcare can safeguard the confidentiality, integrity, and availability of medical data while strengthening overall cybersecurity resilience. The standard provides practical guidance across various domains, including asset management, access control, cryptographic safeguards, physical and environmental security, and system development practices.

The Indonesian regulatory environment further supports this initiative. Regulations such as the Ministry of Communication and Information Regulation No. 4 of 2016, Government Regulation No. 71 of 2019, and BSSN Regulation No. 8 of 2020 all advocate for the adoption of ISO 27001 among institutions providing public services (kominfo, 2016; BSSN, 2020).

Given these challenges and gaps, this study aims to explore the implementation roadmap for ISO 27001:2022 in Indonesian Regional Government Hospitals. The research specifically addresses three key objectives:

(1) Identifying stages and strategies for ISO 27001:2022 adoption
(2) Assessing the current maturity of existing ISMS frameworks within hospitals
(3) Formulating actionable recommendations to enhance information security governance in alignment with international standards

Related Work

The adoption of ISO/IEC 27001 as a framework for securing healthcare information systems has been widely explored in both domestic and international contexts. This standard serves as the backbone of information security

management by emphasizing the principles of Confidentiality, Integrity, and Availability (CIA) of sensitive data. However, the practical application of the standard often faces challenges, especially in public sector environments such as regional hospitals in developing countries.

Several international studies have examined the intersection of ISO/IEC 27001 with healthcare systems. Conducted a systematization of 49 cybersecurity standards and guidelines, including ISO/IEC 27001, using the NIST Cybersecurity Framework as a baseline. They identified gaps in regulatory clarity, overlaps across documents, and implementation difficulties in the healthcare sector, especially concerning electronic health records and cloud services. Similarly, (Zarei and Sadoughi, 2016).) reported inconsistent implementation of ISMS across Iranian hospitals, highlighting governance fragmentation and limited staff awareness as key barriers.

From a technical standpoint, Ali et al. (2023) proposed an AI-based compliance model to automate ISO 27001 audits in healthcare infrastructure, showcasing the potential of machine learning for real-time risk monitoring. Meanwhile, Yang et al. (2022) integrated ISO controls with blockchain and attribute-based encryption to enhance the security of medical data sharing frameworks, particularly addressing the need for fine-grained access control.

In the Indonesian context, Maraqonitatilla and Palupi (2023) evaluated a regional public hospital's ISO/IEC 27001:2013 compliance level and found significant gaps in documentation, incident response, and asset control. Likewise, Medina and Rahadian (2023) applied ISO/IEC 27005 for risk assessment in local government infrastructures, identifying vulnerabilities stemming from the absence of formal SOPs and inconsistent asset inventories.

Cross-framework integrations have also been explored. For instance, Nawir et al. (2022) combined ISO/IEC 27001 with COBIT 2019 to develop a hybrid governance model for smart tourism, suggesting a similar approach could be beneficial for health IT governance. Utilized OCTAVE Allegro alongside ISO controls to generate 42 mitigation strategies in a state-owned enterprise, reinforcing the relevance of structured risk assessments. These efforts highlight that applying ISO standards in silos may be insufficient without governance and contextual adaptation.

Recent research by Restiana et al. (2022) on PT Bank Jago underscored the role of information security governance in enabling digital transformation, indirectly aligning with ISO/IEC 27001 principles. Lucia et al. (2024) also used the KAMI Index, mapped to ISO 27001:2022, to assess readiness and highlighted deficiencies in cloud security and monitoring.

In summary, despite the wide adoption of ISO/IEC 27001 and related standards, both international and national studies reveal persistent challenges in healthcare institutions ranging from governance and training gaps to technical compliance issues. This study builds upon these insights by offering a detailed risk assessment of Indonesian Regional Government Hospitals based on ISO/IEC (2022), aiming to provide actionable recommendations for enhanced cybersecurity posture.

Workflow of the Research

This research employed a single-case study design focused on a selected regional public hospital that had implemented a Hospital Management Information System (SIMRS). The hospital was chosen due to its high reliance on digital systems and observable issues related to information security implementation. A qualitative descriptive approach was applied to deeply examine technical, organizational, and policy-related aspects of the hospital's information security.

The research process was structured into several sequential stages as illustrated in Figure 4, consisting of the following steps:

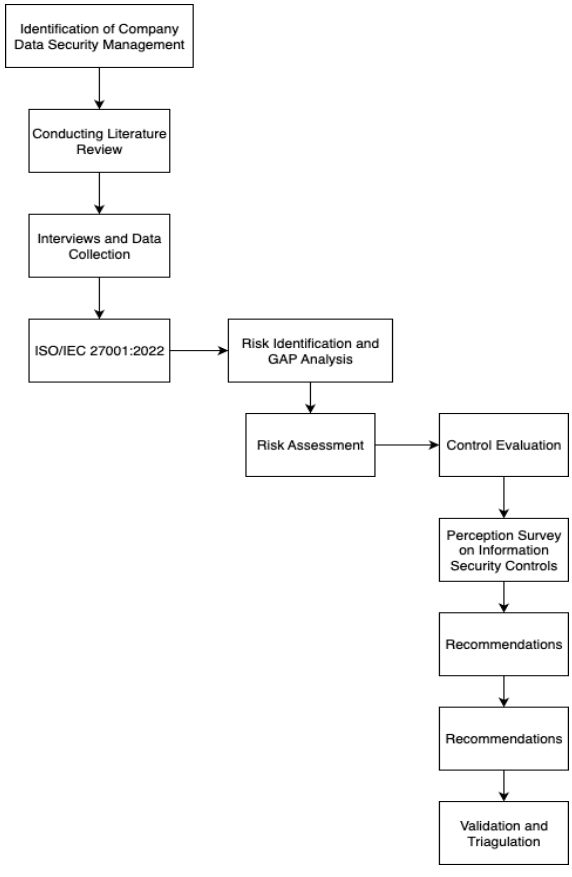

Fig. 4: Research Workflow

1. Preliminary Study and Context Understanding: An initial assessment was carried out to understand the hospital environment, identify key stakeholders, and define the evaluation scope. This stage included informal discussions and a background review of the SIMRS system used
2. Literature Review: A comprehensive literature review was conducted, covering relevant regulations and academic studies related to ISO/IEC 27001, ISO/IEC 27005, risk assessment frameworks, and healthcare-specific information system case studies. This provided the theoretical foundation for the research
3. Data Collection: A triangulated approach was used to ensure data validity, employing

- Semi-structured interviews with IT personnel, SIMRS end-users (both administrative and medical staff), and hospital management
- Direct observations of system usage, physical infrastructure, user behavior, and compliance with SOPs
- Document analysis, including IT policies, SOPs, organizational charts, access logs, and incident reports

4. Risk Identification and Asset Classification
5. In accordance with ISO/IEC 27005, this phase involved identifying critical information assets, potential threats, and existing vulnerabilities. Supporting data included network diagrams, asset inventories, and operational records
6. Risk Analysis and Evaluation Risks were assessed using a 5×5 matrix based on two criteria: Likelihood and *impact*. The resulting risk scores were classified into Low, Medium, or High categories. These scores served as the basis for selecting appropriate treatment controls, as recommended in Clause 6.1.3 of ISO/IEC 27001:2022
7. GAP Analysis and ISO 27001 Control Mapping.
8. The current implementation was benchmarked against the 93 controls listed in Annex A of ISO/IEC 27001:2022. Controls were classified as:

- Fully implemented
- Partially implemented
- Not implemented The assessment utilized the Plan–Do–Check–Act (PDCA) cycle to evaluate ISMS maturity and identify areas for improvement

9. Recommendation Formulation: Based on the identified risks and control gaps, tailored recommendations were developed to enhance the hospital's ISMS maturity, increase regulatory compliance, and strengthen data security practices
10. Validation and Triangulation: To ensure that the proposed recommendations effectively address the identified issues, a validation phase was conducted using a questionnaire distributed to key stakeholders (e.g., IT personnel and hospital management). The purpose of this questionnaire was to verify whether the recommendations align with the problems uncovered during risk identification and gap analysis

Furthermore, triangulation was performed by comparing interview results with observational and documentary evidence. Any inconsistencies between policy documents and real-world practices were carefully analyzed to strengthen the credibility and reliability of the research findings.

Research Design

A single-case study was conducted at a selected regional public hospital that had adopted a Hospital Management Information System (SIMRS). The site was selected based on its high dependence on digital systems and observable shortcomings in information security implementation. The qualitative design enabled the researchers to deeply explore organizational behavior, policy implementation, and technological infrastructure.

Data Collection Techniques

Data for this study were collected using three main techniques, semi-structured interviews with IT personnel, SIMRS end-users including both medical and administrative staff and hospital management; direct observations of system usage behavior, device security, physical infrastructure, and compliance with established procedures; and document analysis, which included reviewing information security policies, IT organizational structures, Standard Operating Procedures (SOPs), access logs, and incident reports. The triangulation of these methods enhanced the validity and reliability of the research findings by allowing cross-verification of data from multiple sources and perspectives (Creswell and Poth, 2017).

Evaluation Framework and ISO Implementation Stages

The evaluation was guided by the ISO/IEC 27001:2022 standard, with a focus on the 14 control domains listed in Annex A. To ensure structured analysis, the Plan Do Check Act (PDCA) model was applied as a framework for reviewing the organization's ISMS maturity:

1. Plan: This phase involved identifying the ISMS context, defining the scope, identifying stakeholders, and conducting risk identification and assessment related to information assets and threats.

This also included a review of relevant policies and mapping current practices against ISO 27001 control requirements

2. Do: This stage is related to the implementation of selected Annex A controls, such as access control mechanisms, physical and environmental security, and staff awareness programs. Although controls were not deployed directly by the researcher, this phase assessed the extent of implementation already in place at the hospital.
3. Check: The evaluation of ISMS performance was conducted using a gap analysis. Each control was scored as "fully implemented," "partially implemented," or "not implemented." This allowed identification of implementation gaps and priority areas for corrective actions
4. Act: Recommendations were developed based on the findings to support continuous improvement. Suggestions included formalizing incident response procedures, improving risk communication, and conducting regular security awareness training

The use of the PDCA model helped ensure that both technical controls and organizational factors were considered in alignment with ISO 27001 strategic objectives.

Risk Assessment Process

A structured risk assessment matrix was used, following the guidelines of ISO 27005 and (ENISA 2019), to identify and prioritize information security threats within the hospital (Table 1). Each identified risk was evaluated based on two key parameters: Likelihood, which refers to the probability that a threat could occur, and impact, which represents the potential severity of consequences if the risk were to materialize. This approach enabled systematic risk classification and informed the prioritization of appropriate mitigation measures. The Risk Score was calculated using the formula:

$$\text{Risk Score} = \text{Likelihood} \times \text{Impact}$$

The results of the risk assessment were categorized into three levels: Scores ranging from 1 to 4 were classified as Low Risk, 5 to 14 as Medium Risk, and 15 to 25 as High Risk. In line with Clause 6.1.3 of ISO/IEC 27001:2022, the selection of risk treatment controls was conducted by identifying and implementing relevant security controls from Annex A to reduce risks to acceptable levels. Each control was carefully mapped to its corresponding threat to ensure proper alignment between identified risks and mitigation strategies.

Validation and Triangulation

To enhance the credibility and applicability of the research findings, both methodological triangulation and stakeholder validation were conducted. Interview responses were compared against observational findings and document analysis to identify discrepancies between formal procedures and actual practices.

Additionally, a validation phase was carried out using a structured questionnaire distributed to IT staff and management stakeholders. This instrument aimed to assess whether the proposed recommendations adequately addressed the identified security issues. The feedback obtained served to refine and confirm the feasibility and relevance of the improvement suggestions.

Table 1: Risk Assessment Matrix

Likelihood / Impact	1 (Very Low)	2 (Low)	3 (Moderate)	4 (High)	5 (Very High)
1 (Rare)	1 (Low)	2	3	4	5 (Medium)
2 (Unlikely)	2	4	6	8	10
3 (Possible)	3	6	9 (Medium)	12	15
4 (Likely)	4	8	12	16	20
5 (Very Likely)	5 (Medium)	10	15	20	25 (High)
Likelihood / Impact	1 (Very Low)	2 (Low)	3 (Moderate)	4 (High)	5 (Very High)
1 (Rare)	1 (Low)	2	3	4	5 (Medium)
2 (Unlikely)	2	4	6	8	10
3 (Possible)	3	6	9 (Medium)	12	15
4 (Likely)	4	8	12	16	20
5 (Very Likely)	5 (Medium)	10	15	20	25 (High)

Results and Discussion

This section presents a comprehensive and detailed analysis of information security risks in Indonesian regional government hospitals, utilizing both ISO/IEC 27001:2022 and ISO/IEC 27005 frameworks as the primary references (Table 2). The assessment process involved a mixed-method approach combining qualitative and quantitative strategies, including in-depth interviews with key stakeholders (such as IT managers and administrative heads), direct observations of operational practices, review of internal policy documents and SOPs, and a structured validation survey distributed to hospital staff.

Methodological triangulation was employed to ensure data reliability and consistency across multiple data sources. The findings from interviews and document reviews were cross-validated through questionnaire responses, ensuring alignment between perceived practices and actual implementation. Each identified issue or control area was mapped against the relevant ISO/IEC 27001:2022 clause, particularly from Annex A, and its implementation status was assessed using a risk-based approach derived from ISO/IEC 27005.

Risk levels were determined by calculating a composite risk score using two key parameters: The likelihood of threat occurrence and the potential impact on information assets. These values were visualized through a heatmap matrix to enhance clarity and highlight the priority areas for intervention. Additionally, implementation gaps were categorized according to their severity (high, medium, low) and accompanied by targeted mitigation strategies, tailored to the specific operational context of the hospital.

The discussion in this section is structured around eight core domains of information security, ranging from access management and policy governance to vendor compliance and incident response. Each domain is critically analyzed to identify existing vulnerabilities, root causes, and the extent to which current practices deviate from ISO standards. Furthermore, practical and actionable recommendations are provided for each gap, integrating best practices from the PDCA (Plan Do Check Act) cycle and emphasizing the need for a holistic and sustainable Information Security Management System (ISMS). Where relevant, comparative analysis with similar case studies in the healthcare sector is also included to validate the generalizability of the findings.

To further illustrate the distribution of risks identified through the assessment, a risk heatmap was generated. This visual representation plots the level of risk based on two key dimensions: Likelihood (the probability of occurrence) and impact (the severity of consequences if the risk materializes). Each risk item was assigned a score ranging from 1 to 5 for both likelihood and impact based on ISO/IEC 27005:2022 guidelines. The resulting product (risk score) determines the risk level category: Very low, low, moderate, high, or very high. This heatmap provides a clear overview of which risk categories fall into critical zones and helps prioritize control implementation efforts. For example, access control weaknesses and outdated security policies appear in the "very likely–high impact" quadrant, signalling an urgent need for mitigation. In contrast, vendor-related issues with lower scores occupy the "possible low impact" zone, indicating moderate concern. This visual aid supports decision-makers in efficiently allocating resources and formulating risk-based improvement strategies.

Comparative Analysis and Insights

Compared to best practices outlined in ISO/IEC 27001:2022, the hospital's ISMS implementation reveals significant gaps, particularly in areas of access control, security policy, and personnel awareness.

Table 2: Risk Assessment Summary Based on ISO 27005 Scoring Matrix

Risk Category	Issue Description	Likelihood (1–5)	Impact (1–5)	Risk Score	Risk Level
Security Policy	Policy is outdated, lacks legal alignment	4	5	20	High
Access Management	Shared accounts, no MFA	5	5	25	High
Training & Awareness	No security awareness training	4	4	16	High
Backup System	Manual backups, no UPS	4	4	16	High
Incident Reporting	Unstructured, via WhatsApp	3	3	9	Medium
Audit & Evaluation	No regular audit	2	4	8	Medium
Email & Comms	Use of personal email	3	4	12	Medium
Vendor Management	No audit of vendors	2	3	6	Medium

This is aligned with similar findings from regional hospital studies in Southeast Asia, which highlight that ISMS maturity in public healthcare remains low without mandated governance (Kim and Lee, 2024). For example, the use of shared accounts contradicts control A.5.15 on identity management, and the lack of regular audits undermines A.5.36. These comparisons underscore a systemic need for policy enforcement and training reinforcement.

Recommendations for Risk Mitigation

Based on the risk assessment and gap analysis conducted using the ISO/IEC 27001:2022 and ISO/IEC 27005 frameworks, several key recommendations have been formulated to strengthen the hospital's information security posture:

1. Policy Update and Enforcement: Revise and update the hospital's Information Security Policy to align with current threats and regulatory requirements, such as Indonesia's Personal Data Protection Law. Ensure periodic reviews and formal enforcement mechanisms are in place to monitor compliance
2. Access Control Improvement: Eliminate shared account practices by enforcing individualized login credentials and implementing Role-Based Access Control (RBAC). Introduce Two-Factor Authentication (2FA) to add an additional security layer, particularly for administrative-level access
3. Security Awareness and Training Programs: Establish structured and recurring information security training sessions for all hospital staff. Topics should include phishing awareness, password hygiene, and data handling best practices. Monitor training effectiveness through pre/post assessment surveys
4. Backup and Recovery Strategy: Improve the robustness of backup procedures by automating regular backups and validating data restoration capabilities through scheduled drills. Ensure that backup media are encrypted and securely stored in compliance with ISO controls A.12.3 and A.17.1
5. Incident Management Protocols: Formalize an incident response plan with clear roles, escalation paths, and post-incident review mechanisms. Integrate the plan with communication tools (e.g., WhatsApp for immediate alerts) while maintaining documentation for forensic analysis
6. Vendor Risk Management Conduct regular audits of third-party service providers and enforce Service Level Agreements (SLAs) that include information security clauses. Evaluate vendors using a risk-based approach prior to onboarding
7. Asset Inventory and Classification: Establish a centralized IT asset management system and classify all information assets based on sensitivity and criticality. Tagging assets and defining protection requirements will enable better control over data flows and access rights
8. Monitoring and Continuous Improvement: Adopt a continuous improvement cycle based on the PDCA (Plan Do Check Act) model. Regularly review control effectiveness, perform internal audits, and utilize performance metrics such as incident frequency, MTTR (Mean Time To Resolve), and user compliance rates

Validation and Triangulation

To ensure the accuracy and generalizability of the results, a rigorous validation process was conducted using methodological triangulation. This involved:

- In-depth interviews with five key hospital stakeholders, including the IT Manager, system administrator, and medical staff responsible for data handling and system usage
- Direct observations of operational workflows, focusing on access control practices, data entry routines, physical server security, and backup procedures
- Document analysis covering internal SOPs, security policies, vendor agreements, and audit logs
- Expert review from an external certified ISO/IEC 27001 auditor, who evaluated the mapped control implementations and risk gaps for accuracy and practical feasibility
- Structured validation survey, distributed to 20 respondents comprising IT personnel, administrative staff, and department heads. The survey measured their perceptions regarding the presence and effectiveness of key ISO 27001 control implementations, using a 5-point Likert scale

Agreement Distribution Results: The survey results revealed a consensus among participants regarding the identified gaps and the relevance of the proposed recommendations. Specifically:

- 85% of respondents strongly agreed or agreed that access control issues were critical and required urgent resolution
- 75% acknowledged weaknesses in data backup and recovery practices
- 90% supported the need for periodic staff training and improved awareness programs
- 80% agreed that vendor risk management practices were not clearly defined or enforced
- 70% rated the current policy documentation as outdated or insufficient

These findings confirm the alignment between the

perceived risks by staff and the empirical findings from interviews and observations. Moreover, the consistency of responses across different stakeholder groups highlights the institutional relevance of the issues identified.

This comprehensive triangulation process enhances the validity and reliability of the assessment and ensures that the proposed recommendations are not only technically sound but also supported by those directly involved in operational activities.

Conclusion

This study evaluated the current state of information security in Indonesian Regional Government Hospitals using the ISO/IEC 27001:2022 framework. The findings revealed that most identified issues fell into high- and medium-risk categories, particularly in the areas of access management, outdated security policies, staff awareness, and system backup procedures. These weaknesses threaten the confidentiality, integrity, and availability of patient data as well as hospital operational continuity. By mapping the risks against Annex A controls and applying the PDCA model, this study formulated practical recommendations to strengthen governance, enhance human resource readiness, and integrate technical and administrative security measures.

Despite its contributions, this study has several limitations. First, it was conducted as a single-case study at one regional hospital, which limits the generalizability of the findings to other healthcare institutions. Second, the methodology primarily relied on qualitative techniques such as interviews, observations, and document analysis—supported by limited survey validation, without the inclusion of statistical modeling or quantitative verification. Third, the assessment scope was confined to the ISO/IEC 27001:2022 framework and did not include other complementary standards such as COBIT 2019 or the NIST Cybersecurity Framework, which could offer a more comprehensive perspective.

Future research should address these limitations by conducting multi-case or comparative studies across multiple hospitals, including both public and private healthcare facilities, to enhance the generalizability of the findings. Quantitative approaches, such as Structural Equation Modeling (SEM) or statistical validation, could complement the qualitative insights and provide stronger empirical evidence. Additionally, exploring hybrid frameworks for example, integrating ISO/IEC 27001 with COBIT 2019 or NIST CSF would enrich the analytical scope and yield more holistic recommendations for healthcare information security in Indonesia. Cross-cultural or longitudinal studies are also encouraged to examine how ISMS maturity and risk management evolve across different healthcare environments over time.

In summary, this study contributes both practically and academically by demonstrating how ISO/IEC 27001:2022 can be applied to assess and mitigate information security risks in Indonesian regional government hospitals. It provides contextual insights to strengthen ISMS implementation in the healthcare sector and establishes a foundation for future research to expand, validate, and refine these findings.

Acknowledgment

The authors gratefully acknowledge Bina Nusantara University (BINUS) and the Master of Information Systems Management Program for institutional support, as well as the management and staff of the participating regional public hospital for permitting interviews, observations, and document access. We also thank the academic supervisor for constructive guidance throughout the study. Any opinions, findings, and conclusions expressed in this article are solely those of the authors and do not necessarily reflect the views of the acknowledged parties.

Funding Information

The publication of this article was funded by Bina Nusantara University (BINUS), under the Master of Information Systems Management Program, as part of its commitment to supporting research and scientific publication by graduate students.

Author's Contributions

Deo Alif Alfitrah: Conceptualized and designed the research framework, conducted the data collection process through interviews and document analysis, and performed the comprehensive risk evaluation based on ISO/IEC 27001:2022 and ISO 27005 standards. He was also responsible for drafting the initial manuscript and integrating feedback during the writing process.

Nilo Leegowo: Contributed to the methodological development and refinement of the risk analysis. He was actively involved in reviewing the results, editing the manuscript, and providing critical revisions to improve the academic clarity and technical accuracy of the final version.

Ethics

This study was conducted using a qualitative case study approach without involving any medical interventions or direct experimentation on human subjects. All data were collected through interviews and institutional documents with prior permission from the hospital. The research adhered to academic ethical standards, maintaining the confidentiality of institutional information and respecting participant anonymity.

References

Ali, M., Ishaq, M., & Hussain, A. (2023). An automated compliance framework for critical infrastructure security through artificial intelligence. *International Journal of Advanced Computer Science and Applications*, 14(1), 10–19. https://doi.org/10.14569/IJACSA.2023.0140113

BSSN. (2020). Badan Siber dan Sandi Negara Republik Indonesia *Peraturan Kepala BSSN Nomor 8 Tahun 2020 tentang Strategi Keamanan Siber Nasional*.

Creswell, J. W., & Poth, C. N. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.*

ENISA. (2019). *Risk Management: Implementation Principles and Inventories for Risk Management/Assessment Methods and Tools*.

ISO/IEC. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements. Geneva: International Organization for Standardization.

Kim, J., & Lee, H. (2024). Improving medical ISMS with dynamic threat modeling. In *Journal of Computer Security* (Vol. 32, Issue 3, pp. 309–331).

Kominfo. (2016). *Peraturan Menteri Komunikasi dan Informatika No.*

Lucia, J. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi keamanan teknologi informasi menggunakan indeks keamanan informasi 5.0 dan iso/eic 27001:2022. *Jurnal Saintekom*, *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Medina, A., & Rahadian, B. (2023). Analisis penilaian risiko keamanan informasi berdasarkan ISO 27005 untuk persiapan sertifikasi ISO 27001. *Jurnal Keamanan Informasi (Indonesia)*, *4*(1), 78–90. https://doi.org/10.26593/jrsi.v12i2.6315.155-164

Maraqonitatilla, M., & Palupi, G. S. (2024). Analisis Tingkat Keamanan Informasi Pada RSUD Dr. R. Sosodoro Djatikoesoemo Bojonegoro Menggunakan Indeks KAMI Berdasarkan ISO 27001:2013. *Journal of Emerging Information Systems and Business Intelligence (JEISBI)*, *5*(2), 66–72. https://doi.org/10.26740/jeisbi.v5i2.59469

Nawir, M., AP, I., & Wajidi, F. (2022). Integrasi framework ISO 27001 dan COBIT 2019 pada smart tourism. *Jurnal Teknologi Dan Sistem Informasi (Indonesia)*, *6*(2), 55–65.

Nugroho, A., & Legowo, N. (2022). Risk assessment using ISO 27001:2022 at IT company. *Jurnal Teknologi Dan Sistem Informasi*, *10*(2), 115–125.

Permenkes, RI. (2025). *Peraturan Menteri Kesehatan No. 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit.*

Undang-Undang Republik Indonesia. (2023). *Undang-Undang No. 17 Tahun 2023 tentang Kesehatan*. Pemerintah Republik Indonesia.

Restiana, R., Sitio, B., & Situmorang, P. (2022). Transformasi digital PT Bank Jago Tbk. *Jurnal Ekonomi Dan Teknologi Digita*, *4*(1), 112–120.

Shipu, D. (2023). Integrating IT in healthcare: Developments and challenges. *World Journal of Advanced Research and Reviews*, *19*(1), 455–463.

Yang, Y., Liu, Y., Zhang, X., Zhao, S., & Wei, J. (2022). Medical data sharing using cryptosystem and blockchain. In *Wireless Communications and Mobile Computing, Article: Vol. ID* (p. 9014737).

Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk management and healthcare policy*, 75-85. https://doi.org/10.2147/RMHP.S99908