



Equivalent: Jurnal Ilmiah Sosial Teknik

Volume 8, Issue 3, 1266-1281

e_ISSN: 2775-0833

<https://jurnalequivalent.id/index.php/jequi/index>

DOI: doi.org/10.59261/jequi.v8i3.387

Integrated Healthcare IT Risk Management in a Hospital Setting: A Case Study of ISO 31000 and NIST SP 800-30 Implementation at Murni Teguh Tuban Bali Hospital

Leo Denny Hartanto*

Universitas Bina Nusantara,
Indonesia

Benfano Soewito

Universitas Bina Nusantara,
Indonesia

***Corresponding author:**

Leo Denny Hartanto, Universitas Bina Nusantara, Indonesia

✉ leodennyhartanto@gmail.com

Article Info:

Article history:

Received: June 25, 2026

Revised: July 23, 2026

Accepted: August 05, 2026

Keywords:

Cybersecurity; Hospital Information System; Information Technology Risk Management; ISO 31000; NIST SP 800-30.

Abstract

Background: Digital transformation in the healthcare sector has significantly increased the use of systems such as Hospital Information Systems (HIS), Electronic Medical Records (EMR), and technology infrastructure. This reliance increases risks of operational disruptions, cyber threats, and data breaches.

Objective: This study aims to develop an integrated IT risk management framework that combines ISO 31000 and NIST SP 800-30, and to examine how this integration supports regulatory compliance and hospital accreditation requirements.

Methods: A case study was carried out at Murni Teguh Tuban Hospital in Bali, Indonesia. Data were collected through interviews with seven informants from management and the IT unit, questionnaires, and direct observations. Risks were scored using a likelihood × impact matrix validated through source triangulation.

Results: ISO 31000 was applied as the governance framework while NIST SP 800-30 guided the technical assessment at every stage. The results show that three key assets are categorized as having very high-risk levels, namely systems (20), external services and vendors (16), and hardware (15). In terms of threats, operational risks are the most significant (20). The evaluation also highlights several gaps, including the absence of Multi-Factor Authentication (MFA), lack of regular IT audits, and insufficient security monitoring. To address these issues, mitigation strategies focus on strengthening access controls, performing regular updates, and implementing a Disaster Recovery Plan (DRP).

Conclusion: The combining of ISO 31000 and NIST SP 800-30 offers a more balanced approach, helping improve security, system resilience, and service continuity.

To cite this article: Hartanto, L. D., & Soewito, B. (2026). Integrated Healthcare IT Risk Management in a Hospital Setting: A Case Study of ISO 31000 and NIST SP 800-30 Implementation at Murni Teguh Tuban Bali Hospital. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(3), 1266-1281. <https://doi.org/10.59261/jequi.v8i3.387>

INTRODUCTION

Information technology is the integration of hardware, software, and telecommunications networks used to process and distribute information (Artamevia et al., 2024). The digital transformation in the healthcare sector has led to the increasingly widespread use of information systems, making effective governance essential to support improvements in service quality (World Health Organization, 2025). Digitalization is also encouraging hospitals to use Hospital Information Systems (HIS) in various operational activities, ranging from patient registration, clinical and non-clinical services, and electronic medical record management to the implementation of telemedicine services (Basri, 2024; Effendy, 2024). This also helps reduce

reliance on manual processes that are prone to human error ([Ariyanti, 2023](#)).

This growing dependency creates a direct causal chain: because patient registration, clinical documentation, diagnostics, pharmacy, and billing are all executed through HIS and EMR, any disruption to these systems immediately halts or degrades clinical and administrative services. Consequently, the higher the operational dependency on HIS/EMR, the greater the potential impact of IT failures, which makes a systematic and structured risk management framework a necessity rather than an option for hospitals.

The rise of digitalization in the healthcare sector has been accompanied by an increase in cyber threats. In May 2021, approximately 279 million records of Social Security Agency for Health enrollees were reported to have been leaked and sold in Indonesia ([Permadi, 2025](#)). The Indonesian National Cyber and Cryptography Agency recorded more than 1.6 billion cyberattacks in 2021 ([Rahmawati, 2025](#)), and a 2024 report indicates over 330 million network anomaly incidents throughout that year ([BSSN, 2025](#)).

The urgency of this issue extends beyond data loss. Healthcare organizations are attractive targets because medical records are a rich source of valuable data while sector defenses remain comparatively weak ([Coventry & Branley, 2018](#); [Kruse et al., 2026](#)). Cybersecurity incidents in hospitals have been shown to disrupt clinical operations directly; the WannaCry ransomware attack on the UK National Health Service in 2017, for example, forced the cancellation of approximately 19,000 appointments and demonstrated that cyber risk in healthcare is ultimately a patient-safety risk ([Ghafur et al., 2019](#); [Rajput et al., 2025](#)). Systematic reviews further confirm that threats to healthcare information systems are increasing in both frequency and sophistication, so hospitals need structured, standards-based risk management rather than ad hoc technical fixes ([Jalali & Kaiser, 2018](#); [Kruse et al., 2017](#); [Salama et al., 2024](#)).

In addressing these risks, healthcare facilities in Indonesia operate within a strict regulatory framework. Indonesian law No. 17 of 2023 on Health, Article 395, stipulates the obligation of hospitals to protect patient information and ensure the security of information technology systems ([P. Indonesia, 2023](#)). This regulation is reinforced by Indonesian law No. 27 of 2022 on Personal Data Protection (PDP Law), which classifies health data as sensitive personal data, meaning its management must adhere to the principles of legality, compliance, and security ([P. Indonesia, 2022](#)).

In addition to legal regulations, hospitals are also required to meet quality standards and accreditation requirements. The National Hospital Accreditation Standards, as stipulated in Ministerial Decree No. 1596 of 2024, require information system risk management, incident response plans, and periodic information security audits ([Kemenkes RI, 2024](#)). Internationally, the Joint Commission International (JCI) Accreditation Standards for Hospitals, 8th edition, 2024, also emphasizes the importance of managing health technology risks and information security, including access controls, cyber threat mitigation, and the sustainability of technology-based critical systems ([Quicho, 2024](#)). Hospitals need to implement preventive measures to protect patient data ([Vantisssha, 2022](#)).

To address technical challenges while meeting compliance requirements, it is necessary to implement risk management practices based on international standards. ISO 31000 serves as a framework that supports a comprehensive risk management process, from identification to mitigation ([ISO, 2025](#)). On the other hand, NIST SP 800-30 provides a more technical approach to assessing risks in information systems, ranging from identifying assets and analyzing potential threats to assessing possible impacts ([NIST, 2012](#)). The combination of these two standards results in more comprehensive risk management for hospitals.

Several previous studies have discussed the implementation of IT risk management using various frameworks. The NIST SP 800-30-based approach, for example, is often used to identify technical threats, such as risks to servers resulting from power or network outages ([Rahmi & Ikhwan, 2025](#)). On the other hand, ISO 31000 is more commonly used for strategic risk mapping, particularly in the context of hospital information systems. Beyond the technical aspect, several studies also emphasize that human factors and managerial aspects play a significant role as sources of risk. In fact, some research proposes an integrative approach by combining multiple standards to ensure risk analysis results are more thorough and comprehensive ([Artie et al., 2025](#); [Basri & Ayu, 2024](#); [Putra & Soewito, 2023](#); [Wahdah & Soewito, 2022](#)).

When these studies are examined critically, each shows specific strengths and limitations. Rahmi and Ikhwan (2025) applied ISO 31000 and NIST 800-30 to a hospital information system and produced detailed technical risk registers, but did not connect the results to regulatory or accreditation obligations. Wahdah and Soewito (2022) combined four frameworks for a financial application, demonstrating methodological breadth, yet a four-framework design is difficult to replicate in resource-constrained hospitals. Putra and Soewito (2023) integrated ISO 27005 and NIST SP 800-30 in the insurance sector, showing that framework pairing improves assessment depth, but the model was not tested in a clinical environment with patient-safety implications. Artie et al. (2025) assessed a government data center and emphasized asset-based analysis without addressing the service-continuity requirements typical of hospitals. Taken together, the research gap is clear: no prior study has operationalized a combined ISO 31000 and NIST SP 800-30 model inside a hospital while simultaneously mapping the process to health regulations and to national and international accreditation standards.

However, previous research has generally focused on risk identification and assessment without fully integrating governance aspects, regulatory compliance (Rahmi & Ikhwan, 2025), and accreditation standards. Furthermore, the relationship between the risk management process and compliance with regulations and hospital accreditation standards has not yet been discussed in depth (Utomo, 2022). This indicates that a model is needed that is not only capable of identifying risks but can also help align IT governance with applicable regulations and operational practices in hospitals.

Murni Teguh Tuban Bali Hospital is a Type C private hospital that has been operating since December 12, 2021, in Tuban Kuta, Badung, Bali, Indonesia, and is part of the Murni Teguh Hospitals Group. The hospital has implemented EMR, HIS, radiology systems, and laboratory systems; however, reliance on these technologies creates IT risks, necessitating systematic risk management in accordance with regulations and accreditation standards.

This study proposes a model that combines ISO 31000 and NIST SP 800-30, integrating strategic and technical approaches to IT risk management. Unlike previous studies, this model not only focuses on risk assessment but also links it to governance aspects, regulatory compliance, and accreditation standards. Through this approach, it is hoped that a more systematic and easily implementable framework can be developed, thereby supporting information security, enhancing system resilience, and ensuring the sustainability of IT services in a hospital environment. The novelty of this study therefore does not lie in the mere combination of the two frameworks, but in the context of implementation and compliance integration: every stage of the risk management cycle is explicitly mapped to Law No. 17 of 2023 on Health, the PDP Law No. 27 of 2022, the National Hospital Accreditation Standards (KMK No. 1596 of 2024), and JCI 8th edition requirements, while the risk evaluation mechanism (likelihood × impact scoring validated with the hospital) is applied directly to a live hospital environment. Conceptually, this differs from previous models that stop at risk registers, because compliance evidence and accreditation requirements become both inputs and outputs of the risk management process itself.

Academically, this study contributes an implementation-oriented integration model that enriches the healthcare IT risk management literature, which has largely remained at the conceptual level. Practically, the model provides hospital management with a replicable instrument for building information security governance: risk priorities can be used to allocate security investment, prepare accreditation evidence, and strengthen management oversight of IT risk (Abraham et al., 2019; Bhardwaj et al., 2026; Jalali & Kaiser, 2018; Kruse et al., 2026). For regulators and accreditation surveyors, the model illustrates how compliance obligations can be verified through documented risk assessment artefacts.

METHOD

This study employed a case study approach to analyse information technology risk management in hospitals. The methodology combined ISO 31000 as a strategic framework for organisational risk governance and NIST SP 800-30 as a technical guide for the information system risk assessment process.

This research used a qualitative case study design with an embedded quantitative risk-

scoring component, adopting a mixed descriptive-evaluative approach. The study was conducted from March to May 2026 at Murni Teguh Tuban Bali Hospital.

The combination of these two frameworks was designed to ensure that the risk management process was conducted systematically without methodological overlap, while also supporting compliance with hospital regulations and accreditation standards (I. Hermawan, 2025).

The research stages are presented in Figure 1, which illustrates a structured research flow ranging from data collection and risk analysis to the risk treatment stage.

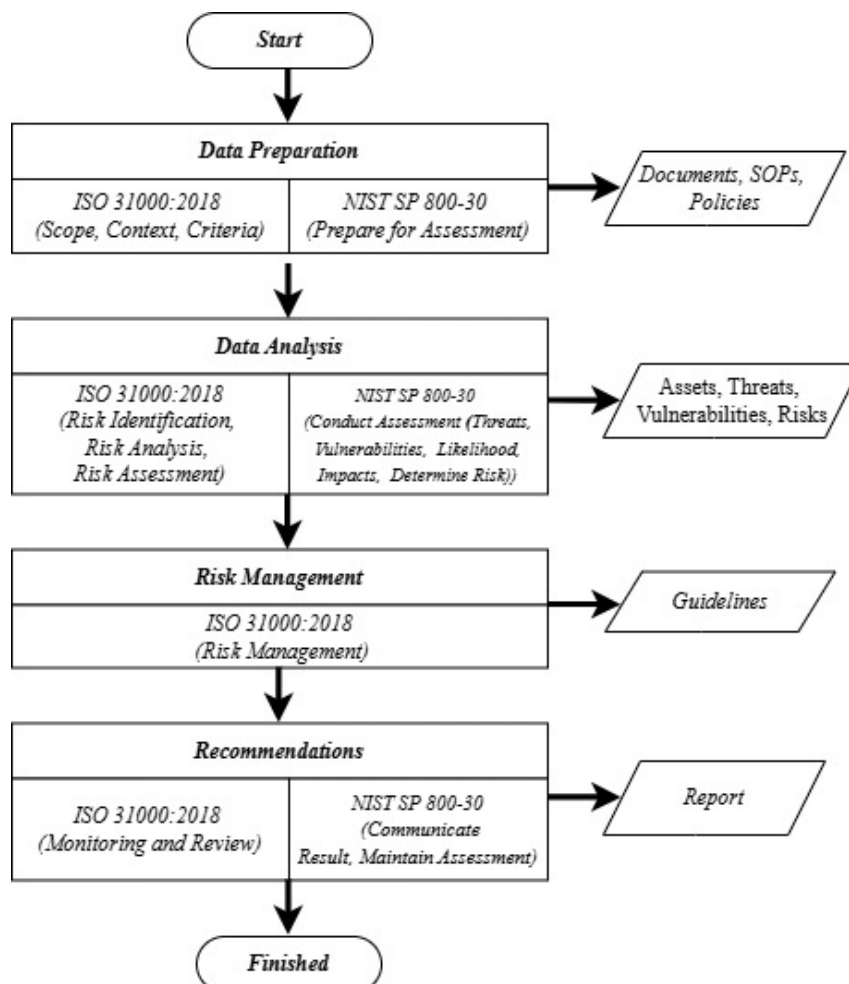


Figure 1. Research Stages

Data preparation involved defining the scope, context, and risk criteria based on ISO 31000, as well as prepare for assessment with NIST SP 800-30. Data collection was conducted through interviews with management and the information technology team, the distribution of questionnaires to relevant units, reviews of policy and procedure documents, and direct observations of the IT infrastructure and network topology mapping. The interviews involved seven purposively selected informants: the Head of the IT Unit, two IT infrastructure staff members, one HIS/EMR administrator, the Head of Quality and Accreditation, one representative from the nursing unit, and one member of hospital management. Questionnaires were distributed to 25 respondents across ten work units that directly interacted with the HIS. The research instruments consisted of a semi-structured interview guide, a risk-assessment questionnaire based on likelihood and impact scales, and an observation checklist.

The data analysis was conducted by identifying critical IT assets and categorizing threats into natural, human, operational, and technical categories, thereby establishing risk priorities as the basis for mitigation (Diahapsari & Riadi, 2022). Interview and observation data were analyzed thematically, while questionnaire data were tabulated to generate likelihood and impact scores. Risk scoring was performed collaboratively by combining expert judgments from the IT team,

hospital incident and downtime records, and direct observation findings. The final scores were determined through consensus between the researchers and the hospital IT team.

To ensure validity, this study applied source triangulation by comparing interview results, policy documents, and observation findings, as well as method triangulation and expert validation. The analysis results and risk scores were confirmed with the hospital IT and quality management teams before being finalized through member checking.

Accurate risk assessments help hospitals minimize disruptions and improve system resilience (Baz et al., 2023). Risk assessment was conducted by measuring the likelihood values presented in Table 1 and the impact values presented in Table 2 using a scale ranging from one to five.

Table 1

Likelihood Scale

Level	Scale	Frequency (Percentage)	Likelihood
1	Very Rarely	0 (0-4%)	May occur more than once every 5 years
2	Rarely	2 (5-20%)	May occur every 2-5 years
3	Sometimes	5 (21-79%)	May occur every 1-2 years
4	Often	8 (80-95%)	May occur several times a year
5	Very Often	10 (96-100%)	Occurs weekly or monthly

Table 2

Impact Scale

Level	Scale	Frequency (Percentage)	Impact
1	Very Low	0 (0-4%)	Slightly disrupts services and can be addressed during routine operations.
2	Low	2 (5-20%)	Significantly disrupts services and threatens the efficiency of certain program aspects.
3	Moderate	5 (21-79%)	Significantly disrupts service operations and results in substantial financial losses.
4	High	8 (80-95%)	Causes major financial and non-financial losses for the hospital organization.
5	Very High	10 (96-100%)	Service disruption lasts more than one week and results in massive financial and non-financial losses for the hospital.

The risk scale in Table 3 are calculated using the formula that multiplies likelihood by impact, resulting in a risk classification ranging from very low to very high.

Table 3

Risk Level Scale

Level	Scale	Risk Level	Risk Color
1	Very Low	1-2	Green
2	Low	3-4	Blue
3	Moderate	5-9	Yellow
4	High	10-14	Orange
5	Very High	15-25	Red

Risk management was determined through an approach that involved avoiding risks, mitigating risks through additional controls, accepting risks within tolerance limits, or transferring risks to third parties (Pohan, 2025). Recommendations were formulated based on risk priorities and the effectiveness of existing controls. The success of the recommendations was evaluated through indicators such as reductions in risk scores, decreases in the number of security incidents, and improvements in compliance with regulations and accreditation standards. Thus,

the combination of ISO 31000 and NIST SP 800-30 formed an adaptive risk management framework that supported the sustainability of IT-based hospital services.

RESULTS AND DISCUSSION

Results

Combination of ISO 31000:2018 and NIST SP 800-30 Rev. 1 Result

Information technology (IT) risk management in the healthcare sector requires an integrated approach that combines national regulations, accreditation standards, and international frameworks such as ISO 31000 and NIST SP 800-30. This approach aims to ensure that risk management not only complies with regulatory requirements but also effectively addresses various potential risks.

Regarding IT risk governance, regulations stipulate that healthcare facilities must ensure the security of data and information systems. Accreditation standards also require the establishment of risk management policies and organisational structures. ISO 31000 serves as a guideline for developing a comprehensive risk management framework, whereas NIST SP 800-30 focuses more specifically on technical risk assessment aspects. Therefore, ISO 31000 is used as the foundation for governance, while NIST SP 800-30 serves as a technical complement.

In defining the scope, regulations and accreditation standards emphasise the importance of data protection and the identification of systems in use. ISO 31000 assists in determining the scope and establishing risk criteria, while NIST SP 800-30 is used to assess the technical conditions of information systems.

During the risk identification phase, regulations promote the prevention of threats to data and healthcare services. ISO 31000 identifies risks from a broader organisational perspective, whereas NIST SP 800-30 examines threats and system vulnerabilities in greater technical detail. These two frameworks complement each other by integrating conceptual and technical perspectives.

Furthermore, during risk analysis, ISO 31000 is used to assess the likelihood and impact of risks, while NIST SP 800-30 provides a more detailed technical analysis of potential threats and vulnerabilities. This integration enables organisations to understand risks more clearly and evaluate them in a measurable manner. In the risk evaluation stage, ISO 31000 establishes assessment criteria based on organisational conditions, whereas NIST SP 800-30 supports the determination of risk levels through more detailed technical evaluations. Consequently, risk priorities can be established more accurately.

In risk treatment, ISO 31000 provides strategic guidance, such as risk reduction, risk avoidance, risk transfer, or risk acceptance, while NIST SP 800-30 offers technical recommendations that can support practical implementation. Regarding service continuity, regulations and accreditation standards require healthcare organisations to establish recovery plans. ISO 31000 supports continuity planning from a management perspective, while NIST SP 800-30 provides technical assessment results that can serve as a basis for decision-making.

Finally, regarding audits and evaluations, regulations require monitoring, oversight, and reporting mechanisms. ISO 31000 guides the process of periodic review and continuous improvement, while NIST SP 800-30 provides documented risk assessment results as supporting evidence for evaluation activities. The integration of ISO 31000 and NIST SP 800-30 can be summarised in Table 4, which presents a comprehensive IT risk management framework for hospitals.

Table 4

Combination of ISO 31000 and NIST SP 800-30 Result

Aspect	Legislation	Accreditation Standards	ISO 31000	NIST SP 800-30	Combination
IT Risk Management	Establishing the obligations of healthcare facilities regarding data security and	The existence of a governance structure and risk management policies	Providing risk management principles and a framework	Does not address aspects of organizational governance	ISO 31000 is used as the foundation for IT risk management policies and

Aspect	Legislation	Accreditation Standards	ISO 31000	NIST SP 800-30	Combination
	information systems		at the organization level		governance structures
Defining Scope and Context	Establishing data and system protection as the institution's responsibility	Requires the identification of hospital systems and services	Define the scope, context, and risk criteria	Performing information system characterization	ISO addresses risk management, while NIST addresses the technical aspects of IT
Risk Identification	Promoting the prevention of threats to health data and services	Requires the identification of operational and technological risks	Identifying risks conceptually	Identifying system threats and vulnerabilities	ISO defines risk, while NIST maps threats and technical vulnerabilities
Technical Risk Analysis	Establishing obligations for mitigating the risk of IT system failure	Requires an analysis of the impact of critical system disruptions	Conducting a risk analysis based on likelihood and impact	Risk control, likelihood, and impact analysis	ISO provides an analytical framework; NIST conducts technical measurements
Risk Assessment and Prioritization	Emphasizing compliance in risk management	Prioritizing Health Care Risks	Evaluating risks based on the organization's criteria	Determining the level of risk	ISO establishes evaluation criteria; NIST calculates risk levels
Risk Mitigation	Focusing efforts on risk reduction and management	Requires a risk mitigation plan	Determining a risk management strategy	Provide technical control recommendations	ISO sets the strategy; NIST provides support through technical recommendations
Services Continuity	Ensuring the continuity of healthcare services	Require a service recovery and continuity plan	Supporting service continuity through risk management	Providing technical input based on risk assessment results	The NIST assessment results serve as the basis for strengthening service continuity within the ISO framework
Audit, Reporting, and Review	Establishing accountability and compliance responsibilities	Requiring regular information system audits	Establishing risk monitoring and review processes	Documenting the results of the risk assessment	ISO sets the evaluation cycle; NIST provides technical evidence.

This combination supports the implementation of systematic risk management while ensuring compliance with data protection regulations and accreditation standards related to the security and sustainability of hospital services. Beyond the conceptual mapping presented in Table 4, each stage was directly implemented at the hospital level: scope definition resulted in the inventory of 860 IT assets across five classifications (Table 5); risk identification identified four threat categories with documented vulnerabilities (Table 6); control analysis evaluated nine existing controls (Table 7); risk evaluation mapped all assets and threats using a 5×5 risk matrix (Table 8); and risk treatment generated prioritized mitigation plans (Table 9). These artefacts provide empirical evidence of the actual implementation of the combined framework at Murni Teguh Tuban Bali Hospital.

Asset Identification and Risk Classification Result

IT assets were identified and classified to determine security priorities based on their importance and associated risk levels. Based on the identification results presented in Table 5, the assets at Murni Teguh Hospital, Tuban, Bali, were categorized into systems, infrastructure, hardware, services and vendors, and non-technical assets, with risk levels calculated as the product of likelihood and impact.

The identification results shown in Table 5 indicate that the system, hardware, and services and vendors classifications represent very high-risk asset categories due to their direct influence on the continuity of the hospital's clinical and administrative operations.

Assets were categorized as critical when they met at least two of the following criteria, each of which establishes a direct relationship between the asset and the hospital's clinical service delivery:

Table 5

Criticality Criteria for IT Assets and Their Link to Clinical Services

Criterion	Link to Clinical Services
Direct support for clinical workflows	The asset executes patient registration, EMR documentation, diagnostics, pharmacy, or billing; failure stops patient services.
Processing/storage of sensitive patient data	The asset holds health data classified as sensitive personal data under the PDP Law; a breach harms patients and exposes the hospital legally.
24/7 availability requirement	Clinical services run continuously; downtime tolerance is low and disruptions cannot wait for office hours.
High interdependency	Failure propagates to other units (e.g., HIS failure disables registration, wards, laboratory, and pharmacy simultaneously).

Tabel 6

Asset Classification and Risk Levels Result

No	Classification	Assets	Total Assets	Function	Likelihood	Impact	Risk Level	Scale
A1	System	Hospital Information System (HIS)	1	Supporting both non-clinical and clinical services.	5	4	20	Very High
A2	Infrastructure	Firewall, Switch, Access Point	92	Providing network connectivity and security for hospitals.	4	3	12	High
A3	Hardware	Servers, Computers, UPS, CCTV, Telephones.	754	Supporting service availability and IT physical security.	3	5	15	Very High
A4	Services & External Vendors	ISP, Cloud, and Email Services.	5	Providing connectivity services and third-party support platforms.	4	4	16	Very High
A5	Non-Technical Assets	IT SOPs, Contracts, and Vendor SLAs.	8	Managing IT governance, compliance, and service continuity.	3	4	12	High

The analysis results show that system assets (A1) received the highest risk score of 20, which is classified as very high risk. This score indicates that disruptions to systems such as the Hospital Information System (HIS) and other supporting applications have a high likelihood of occurrence and may result in significant consequences for both clinical and administrative operations. Hardware assets (A3) are also classified as very high risk, with a score of 15, due to their substantial impact on service continuity in the event of failures involving servers or data storage devices.

Service assets and external vendors (A4) obtained a risk score of 16, indicating the hospital's significant dependency on third parties for connectivity and digital services. Meanwhile, infrastructure assets (A2) and non-technical assets (A5) are categorized as high risk, each with a score of 12. These findings highlight that cybersecurity efforts should prioritize critical systems, essential devices, and external services that support the hospital's operational processes.

The HIS received the highest risk score because it combines the highest likelihood of occurrence with severe operational impact. Downtime incidents have occurred several times within a year (likelihood score = 5), and each disruption directly affects patient registration, clinical documentation, pharmacy services, and billing processes (impact score = 4). From an operational perspective, one hour of HIS downtime requires all units to revert to manual procedures, which are not consistently documented across departments. This condition increases the risk of clinical errors, service delays, and non-compliance with medical record management requirements. Therefore, HIS mitigation is prioritized as the first focus in the risk treatment plan.

Identification of Threats and Vulnerabilities Result

Threat and vulnerability identification aims to determine various types of threats and vulnerabilities that may potentially affect hospital IT assets. As presented in Table 7, threats to IT systems are categorized into four main groups: environmental, human, operational, and technical threats.

Table 7

Classification of Threats and Risk Levels Result

No	Threat Classification	Threat	Impact -ed Assets	Vulnerability	Impact of The Threat	Likelihood	Impact	Risk Level	Scale
B1	Threats to Nature and the Environment	Earthquakes, floods, fires, prolonged power outages.	A1, A2, A3, A4.	No active disaster recovery (DR) site, Internet service provider located on a lower floor, Loose cable connections, Limited UPS capacity.	System crash, hardware failure, data loss, and hardware damage.	2	3	6	Moderate
B2	Threats to humans	Accidental data deletion, password sharing, unauthorized staff access.	A1	Excessive access rights, staff lack of knowledge regarding data security, RBAC controls are not yet stringent	Data loss, unauthorized access, violations of data protection laws.	5	2	10	High
B3	Threats to Operations	Hospital Information System (HIS) error, downtime SOP not available, patch delayed.	A1, A2, A3, A4, A5	The resource server is insufficient; there is no documented SPO downtime; the patch schedule is not regular.	System downtime, service disruptions, and security vulnerabilities	5	4	20	Very High
B4	Threats to Technical	Malware, spam emails, cyberattacks, ISP outages	A1, A3, A4	Out-of-date antivirus software, inadequate cybersecurity training, and limited ISP backup bandwidth.	Operations disrupted, Data encryption, Service outage.	5	2	10	High

The results presented in Table 7 indicate that operational threats (B3) pose the highest risk, with a score of 20, which falls into the “very high” category. This finding suggests that disruptions such as configuration errors, delays in system updates, and the absence of downtime SOPs are likely to occur frequently and may significantly affect service availability and continuity.

Threats arising from human factors (B2) and technical factors (B4) each have a risk score of 10 and are classified as high. The high likelihood of system misuse, password sharing, and

cyberattacks increases the potential for data breaches and operational disruptions.

In contrast, environmental threats (B1) received a score of six and are classified as moderate. Although the likelihood of these threats is relatively lower than that of other threat categories, they still require attention through disaster recovery planning and the strengthening of supporting infrastructure. Overall, these results indicate that operational and human-related threats should receive primary attention in the development of mitigation strategies.

Control Analysis Result

Control analysis aims to evaluate the effectiveness of implemented controls and identify existing control gaps that require further improvement (E. W. Tomlinson, 2024). Table 8, "Control Evaluation," shows that the hospital has established several security controls, including policies for the Hospital Information System (HIS), IT Standard Operating Procedures (SOPs), firewall protection, antivirus software, and username- and password-based access control mechanisms.

Table 8
Control Analysis Result

No	Description	Assets Impact	Threats Related	Vulnerability	Control Analysis
K1	Hospital Information System Policy	A1	B2,B3	Low policy compliance	This policy is reviewed every three years or whenever changes occur.
K2	IT standard operating procedures.	A1, A2, A3	B3, B4	The procedure has not yet been documented in detail	The SOP is reviewed every three years or whenever changes occur.
K3	Daily monitoring of the server room.	A2, A3	B1, B3	Monitoring is conducted in the morning, afternoon, and evening, but not yet on a 24-hour basis.	Proposing changes to the work schedule and additional staff to enable 24-hour monitoring.
K4	Firewall.	A2	B4	No routine firewall monitoring	Monitoring is not yet optimal.
K5	Antivirus.	A1, A3	B4	No routine updates or monitoring	Controls need to be strengthened.
K6	Username and password for the system.	A1	B2, B4	Multi-Factor Authentication (MFA) has not yet been implemented.	Risk of unauthorized access
K7	IT Audit.	A1, A2, A3, A4, A5	B1, B2, B3, B4	The control was not evaluated	The audit has not yet been conducted.
K8	System downtime simulation.	A1, A2; A1, A4	B1, B3	Limited disaster recovery (DR) readiness	The frequency of simulations needs to be increased.
K9	Standard operating procedures for system downtime in each unit.	A1, A5	B3	Standard operating procedures are not available in some units	Proposal for Standardizing Standard Operating Procedures

However, several gaps were identified, including the absence of Multi-Factor Authentication (MFA) implementation; irregular IT audit activities; suboptimal firewall and antivirus monitoring; inconsistent application of downtime Standard Operating Procedures (SOPs) across all units; and manual server room temperature monitoring. These findings indicate that the effectiveness of existing controls remains suboptimal, as several controls have not been evaluated periodically or enhanced in accordance with the identified risk levels. Therefore, improvements to the control system are required to ensure that it becomes more responsive, adaptive, and aligned with a risk-based approach.

Risk Analysis Matrix Result

The Risk Analysis Matrix is designed to map risk levels using a likelihood-and-impact matrix to visually and systematically determine mitigation priorities. Based on the risk matrix presented in Table 9, the “very high” risk category includes systems (A1), hardware (A3), services and vendors (A4), and operational threats (B3). These risks are positioned within the highest-priority quadrant due to their combination of a high likelihood of occurrence and significant potential impact, indicating the need for immediate mitigation measures.

Table 9

Risk Matrix Result

		Impact				
		1	2	3	4	5
Likelihood		Very low	Low	Moderate	High	Very High
1	Very Rarely					
2	Rarely			B1		
3	Sometimes				A5	A3
4	Often			A2	A4	
5	Very Often		B2, B4	A1, B3		

The high-risk category includes infrastructure (A2), non-technical assets (A5), human threats (B2), and technical threats (B4). This distribution indicates that the majority of risks fall within the medium-to-high risk category, thereby requiring systematic and continuous control measures.

Using this matrix, management can more effectively prioritize mitigation efforts based on the urgency and potential impact of each risk on healthcare services.

Risk Management and Mitigation Strategies Result

The risk management and mitigation strategies in this study aim to develop appropriate measures based on the identified risk levels, in accordance with the ISO 31000 risk management principles and the technical analysis results derived from NIST SP 800-30. In general, risk management can be implemented through several approaches, including risk avoidance, risk reduction, risk transfer, and risk acceptance (Pohan, 2025).

The mitigation strategies presented in Table 9 are organized according to the risk level within each category. For operational threats (B3), which are classified as very high risk, the mitigation measures focus on risk reduction strategies, including increasing system capacity, conducting preventive maintenance, implementing regular monitoring, and developing and standardizing procedures related to downtime management and change management.

Human-related threats (B2) and technical threats (B4) are addressed through strengthened risk reduction strategies, including the implementation of role-based access control (RBAC), the adoption of Multi-Factor Authentication (MFA), regular security system updates, and enhanced information security awareness. Specifically, for technical threats, a risk transfer strategy is also applied by optimizing collaboration with vendors and backup service providers.

Environmental threats (B1) are managed through a combination of risk reduction and risk transfer strategies. The implemented measures include the development of a Disaster Recovery Plan (DRP), the utilization of cloud-based backup systems, and improvements in the reliability of supporting infrastructure, such as electrical power and cooling systems. This approach is designed to ensure alignment with the risk levels identified in the previous assessment.

Table 10
Mitigation Strategies by Risk Level Result

No	Threat Classification	Risk Level	Response Strategy	Action Plan
B3	Threats to Operations	Very High	Reducing Risk	System capacity and performance improvements, regular monitoring, preventive maintenance, and standardization of downtime procedures and change management.
B2	Threats to humans	High	Reducing Risk	Implementation of Role-Based Access Control (RBAC), implementation of MFA, evaluation of access rights, and raising awareness of information security.
B4	Threats to Technical	High	Reducing & Transferring Risk	Security system updates, infrastructure monitoring, provision of backup connections, and strengthening of cooperation with vendors.
B1	Threats to Nature and the Environment	Moderate	Reducing & Transferring Risk	Implementation of a Disaster Recovery Plan (DRP), cloud-based backup, improvements to power and cooling reliability, and readiness of emergency response procedures.

Overall, the mitigation strategies formulated are aligned with the identified risk priority levels, thereby supporting the enhancement of the resilience and sustainability of the hospital's information systems.

Discussion

Based on the analysis results, discrepancies remain between the current conditions and the standards that should be achieved. These discrepancies are primarily evident in the areas of security, governance, and system operations.

From a security perspective, the absence of Multi-Factor Authentication (MFA) implementation, limited system monitoring capabilities, and the lack of routine IT audits indicate that existing security controls are not yet fully effective. From a governance perspective, several critical procedures, such as downtime Standard Operating Procedures (SOPs), have not yet been established across all units, and existing documentation remains incomplete. Meanwhile, from an operational perspective, the high level of disruption risk indicates that system readiness requires further improvement.

Compared with previous studies, most research has focused on risk identification and analysis processes, either from a technical perspective using NIST frameworks or from a management perspective using ISO standards. However, these approaches generally have not fully integrated governance, regulatory, and accreditation requirements, resulting in suboptimal implementation within hospital environments.

A more critical comparison reveals differences not only in methodological approaches but also in empirical findings. Rahmi and Ikhwan (2025) identified server and network failures as the dominant risks in hospitals, whereas this study found that operational threats (score 20), driven by the absence of downtime SOPs and irregular patch management, outweigh purely technical threats (score 10). Similarly, previous multi-framework studies reported improved assessment depth (Putra & Soewito, 2023; Wahdah & Soewito, 2022) but did not quantify third-party dependencies. In this study, external services and vendors emerged as very high-risk factors (score 16), a finding that has rarely been emphasized in Indonesian hospital IT risk management literature. These differences demonstrate that contextual factors including hospital type, governance maturity, and vendor dependency significantly influence risk profiles, reinforcing the argument that risk management frameworks should be operationalized according to organizational contexts rather than merely adopted.

The findings of this study demonstrate that IT risk management is insufficient when focused solely on a single dimension, such as technical controls or managerial practices. Therefore, a more comprehensive and integrated approach is required. The model proposed in

this study combines ISO 31000:2018 as the foundation for risk management and NIST SP 800-30 as a technical risk assessment framework while adapting these standards to meet regulatory requirements and accreditation standards. This model extends beyond risk identification by emphasizing practical implementation strategies, including security strengthening, procedural improvement, routine auditing, and enhanced system readiness through a Disaster Recovery Plan (DRP).

The effectiveness of this integrated approach is supported by previous risk management literature. Aven (2016) argues that effective risk management requires both a conceptual governance foundation and a reliable assessment methodology; ISO 31000 provides the former, while NIST SP 800-30 provides the latter (Kruse et al., 2026). Empirical studies in healthcare environments also demonstrate that purely technical controls are ineffective without organizational alignment (Jalali & Kaiser, 2018; Kruse et al., 2026), whereas governance-focused approaches may lack the technical granularity required for prioritizing security safeguards (Abraham et al., 2019; Bhardwaj et al., 2026). In this study, the combination of these frameworks proved effective because NIST-based risk scoring generated auditable evidence (Tables 5–8) that supports ISO-based decision-making while simultaneously fulfilling the documentation requirements of accreditation standards. This approach positions the proposed model within IT governance theory, where risk management functions as a control mechanism that aligns IT operations with organizational objectives and regulatory obligations.

Through this approach, the proposed model is expected to address existing gaps and assist hospitals in improving system security, achieving regulatory compliance, and ensuring the continuity of IT services.

Although individual mitigation measures (MFA, RBAC, DRP, periodic audits, and firewall monitoring) represent established information security practices, the innovation of this model lies in the process through which these controls are derived and prioritized. Each control is selected because it simultaneously (1) reduces a quantified risk score obtained from the NIST-based assessment, (2) addresses a control gap identified in Table 7, and (3) fulfils a specific regulatory or accreditation requirement. For example, MFA is prioritized not merely as a recommended security practice but because it addresses the human-threat risk score of 10, closes control gap K6, and satisfies access-control requirements within accreditation standards. This triple-mapping approach distinguishes the proposed mitigation framework from generic security recommendations.

CONCLUSION

This study aims to integrate ISO 31000 and NIST SP 800-30 as a framework for Information Technology (IT) risk management at Murni Teguh Hospital in Tuban, Bali, Indonesia. Furthermore, this study examines the extent to which the integration of these two standards can support hospital compliance with applicable regulations and accreditation requirements.

The results indicate that integrating these two standards produces a more comprehensive and structured risk management approach. ISO 31000 functions as a strategic foundation for organizational-level risk management, while NIST SP 800-30 provides technical guidance for conducting systematic information system risk assessments.

The analysis revealed that the highest risks are associated with critical systems, including the Hospital Information System (HIS), server infrastructure, and dependence on external vendor services. Quantitatively, the HIS achieved the highest risk score of 20 (very high), external vendor services obtained a score of 16, and operational threats also reached a score of 20. Therefore, mitigation priorities were directed toward strengthening HIS resilience, improving vendor management, and standardizing operational procedures. Additionally, factors such as operational disruptions, human error, and technical failures represent significant sources of risk, particularly concerning service continuity and patient data security.

The resulting recommendations include strengthening access controls through MFA implementation, improving network monitoring capabilities, developing and standardizing downtime-related SOPs, and conducting periodic testing of the Disaster Recovery Plan (DRP). These measures are expected to reduce identified risks while improving the resilience of hospital

information systems.

Future research is recommended to expand the study scope by involving hospitals with different characteristics or incorporating additional information security frameworks. Specifically, future studies may validate the proposed model across various hospital classifications (Types A–D, public and private hospitals) and compare its effectiveness with other frameworks, such as ISO 27005, OCTAVE Allegro, and COBIT 2019, to determine the most efficient combination for compliance-oriented IT risk management. Such investigations are important for strengthening the validity of the findings and expanding the applicability of the proposed framework.

ACKNOWLEDGEMENT

The author would like to thank Murni Teguh Tuban Bali Hospital in Indonesia for its support and for the opportunity provided during the data collection process and the conduct of this study. Appreciation is also given to the management and the information technology team for their active participation in the interviews and for providing the necessary information.

This study did not receive any specific funding from government agencies, private entities, or non-profit organizations. The author also thanks the academic advisor and reviewers for their feedback and constructive suggestions, which helped to improve this research paper.

AUTHOR CONTRIBUTION STATEMENT

Writing initial draft, L. D. H.; Methodology, L. D. H. and B. S.; Formal analysis, L. D. H. and B. S.; Review of analysis results, L. D. H. and B. S. All authors have read and approved the published version of the manuscript.

REFERENCES

- Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business Horizons*, 62(4), 539–548.
- Ariyanti, N., Agushybana, F., & Widodo, A. P. (2023). The Benefits of Electronic Medical Records Reviewed from Economic, Clinical, and Clinical Information Benefits in Hospitals. *Jurnal Kesehatan Komunitas*, 9(1), 190–197. <https://doi.org/10.25311/keskom.vol9.iss1.1420>
- Artamevia, A., Eka, E., Suci, & Dhamanti, I. (2024). Cyber Security Dalam Sistem Informasi Rumah Sakit Indonesia: Kajian Literatur. *Journal Of Social Science Research*, 4, 17410–17421.
- Artie, H. Z., Hilman, M., & Yazid, S. (2025). Penilaian Risiko Keamanan Informasi Pusat Data pada Instansi XYZ. *Jurnal Informatika Ekonomi Bisnis*, 7(2), 270–276. <https://doi.org/10.37034/infeb.v7i2.1160>
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13. <https://doi.org/10.1016/j.ejor.2015.12.023>
- 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. <https://doi.org/10.47738/ijaim.v4i1.70>
- Baz, A., Ahmed, R., Khan, S. A., & Kumar, S. (2023). Security Risk Assessment Framework for the Healthcare Industry 5.0. *Sustainability*, 15(23), 16519. <https://doi.org/10.3390/su152316519>
- Bhardwaj, M., Juneja, Y., & Sidana, N. (2026). Cybersecurity in Healthcare: Risks, Vulnerabilities, and Ethical Imperatives. In *Organ Trafficking Prevention in the Healthcare Sector: Examining the Co-Creation of Cybersecurity Value* (pp. 1–34). IGI Global Scientific Publishing.
- BSSN. (2024). *Lanskap Keamanan Siber Indonesia 2024*. <https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf>
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
- Diahapsari, A., & Riadi, I. (2022). Analysis Risk Assessment on Hospital Management Information System using Octave Allegro Framework. *International Journal of Computer Applications*, 184(24), 27–34. <https://doi.org/10.5120/ijca2022922286>

- Effendy, C. A., Paramarta, V., & Purwanda, E. (2024). Peran Teknologi Informasi, Pengelolaan Sumber Daya Manusia, Dan Sistem Infoemasi Rumah Sakit Dalam Meningkatkan Kinerja Rumah Sakit (Kajian Literatur). *Jurnal Review Pendidikan Dan Pengajaran*, 7(4), 13479–13489. <https://doi.org/https://doi.org/10.31004/jrpp.v7i4.34703>
- Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *Npj Digital Medicine*, 2(1), 98. <https://doi.org/10.1038/s41746-019-0161-6>
- Hermawan, I., Hanggara, B. T., & Perdanakusuma, A. R. (2025). *Manajemen Risiko Sistem Informasi Menggunakan Metode NIST SP 800-30 Studi Kasus Pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo* (Vol. 9, Number 6). <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/14982>
- Indonesia, P. (2022). *Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. <https://doi.org/https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Indonesia, P. (2023). *Undang-undang (UU) Nomor 17 Tahun 2023 tentang Kesehatan*. <https://doi.org/https://peraturan.bpk.go.id/details/258028/uu-no-17-tahun-2023>
- ISO. (2018). *Risk management-Guidelines International Standart ISO 31000:2018*. <https://www.iso.org/standard/65694.html>
- Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, 20(5), e10059. <https://doi.org/10.2196/10059>
- Kemendes RI. (2024). *KMK No. 1596 Tahun 2024 tentang Standar Akreditasi Rumah Sakit*.
- Kruse, C. S., Dolezel, D., & Shanmugam, R. (2026). Cybersecurity in Healthcare: A Systematic Review and Narrative Analysis. In *Applied Clinical Informatics*, 17 (2), 315–328. Georg Thieme Verlag. <https://doi.org/10.1055/a-2865-4206>
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, 25(1), 1–10. <https://doi.org/10.3233/THC-161263>
- NIST. (2012). *Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1)*. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Permadi, D. (2021). *Kominfo: Data Pribadi WNI yang Bocor Identik Data BPJS Kesehatan*. <https://news.detik.com/berita/d-5577462/kominfo-data-pribadi-wni-yang-bocor-identik-data-bpjs-kesehatan>
- Pohan, R. (2025). Adaptasi Manajemen Risiko Pada Sistem Pendidikan Pascapandemi. *Jurnal Media Akademik (JMA)*, 3(12).
- Putra, A. P., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector. In *IJACSA International Journal of Advanced Computer Science and Applications*, 14 (4).
- Quicho, R., Evans, L., Chopp Hinckley, C., & Beth Curran, M. (2024). *Joint Commission International Mission Development Team for the 8th Edition*. <https://www.jointcommissioninternational.org>.
- Rahmawati, D. (2022). *BSSN Temukan 1,6 Miliar Serangan Siber Sepanjang 2021, Mayoritas Malware*. <https://news.detik.com/berita/d-5972491/bssn-temukan-1-6-miliar-serangan-siber-sepanjang-2021-mayoritas-malware>
- Rahmi, T. A., & Ikhwan, M. (2025). Analisis Manajemen Risiko Pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan ISO 31000 dan NIST 800-30 DI RSUD H. Ok Arya Zulkarnain. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(5), 8207–8215. <https://doi.org/10.36040/jati.v9i5.15069>
- Rajput, K., Darzi, A., & Ghafur, S. (2025). Overlooked and under-reported: the impact of cyberattacks on primary care in the UK National Health Service. *The Lancet Digital Health*, 7(7).
- Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: a look at current and future trends. *Computational Intelligence and Blockchain in Complex Systems*, 97–111.

- Utomo, D. K., Santosa, I., & Nutrisha, W. A. (2022). Perancangan Manajemen Informasi Berdasarkan Standar Nasional Akreditasi Rumah Sakit (SNARS) dan Joint Commission International (JCI) Pada Rumah Sakit Gigi Dan Mulut (RSGM) Maranatha. *Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika (JIPi)*, 07(4), 1045–1057. <https://doi.org/https://doi.org/10.29100/jipi.v7i4.3193>
- Vantissha, D., Azizah, A. H., & Arifin, S. (2022). Assessing Hospital Management Information Systems Success Using Human Organization and Technology Fit Model. *Applied Information System and Management (AISM)*, 5(1), 37–44. <https://doi.org/10.15408/aism.v5i1.24738>
- Wahdah, F., & Soewito, B. (2022). manajemen resiko aplikasi keuangan pada perusahaan abc melalui kombinasi NIST SP 800-30, COBIT, PMBOK, dan ISO 31000. *JIKO (Jurnal Informatika Dan Komputer)*, 5(2), 78–83. <https://doi.org/10.33387/jiko.v5i2.4369>
- World Health Organization. (2025). *Global strategy on digital health 2020-2027*. <http://apps.who.int/bookorders>.