 ISSN 2776-8007

Risk Management in Information Systems: Applying ISO 31000:2018 and ISO/IEC 27001:2022 Controls at PMI's Central Clinic

Wahyu Setiawan Basri[1,*], Adinda Laras Ayu[2]

[1]*Department of Information System, Universitas Indonesia, Indonesia*

[2]*Telkom University, Indonesia*

(Received: December 13, 2023; Revised: January 11, 2024; Accepted: March 15, 2024; Available online: April 30, 2024)

Abstract

PMI Main Clinic is a national association organization in Indonesia engaged in health services. PMI Main Clinic has an information system to support its health service process. One of the information systems is the Clinic Management Information System (Smart Klinik), this information system is used to record patients from the beginning of the patient's arrival to register until the patient gets the medicine. PMI Main Clinic has never implemented information system risk management before. If a risk occurs at the PMI Main Clinic, the PMI Main Clinic can suffer huge losses and hamper the health service process. To find out the possible risks that can occur at PMI, the ISO 31000: 2018 method is used and the control standard uses ISO 27001: 2022. It can be seen from the 22 possible risks, there are 4 possible risks with very high levels, 2 possible risks with high risk levels, 10 possible risks with moderate risk levels, and 6 possible risks with low risk levels. The control recommendations used ISO/EIC 27001:2022 from the result Equipment maintenance, Information backup, Protection against malware, Installation of software on operational systems, Monitoring activities, Web filtering, Network's security, Security of network services, Segregation of networks, Secure system architecture and engineering principles.

Keywords: Risk Management, Information System, ISO 31000:2018, ISO 27001:2022, PMI

1. Introduction

In the current era of development, information systems are crucial for the business world, serving as a backbone for the growth of companies or organizations [1]. An information system is defined as a system that involves the collection, processing, storage, analysis, and dissemination of information for specific purposes [2]. Whenever an information system is implemented, there exists potential risk variations that could impede its optimal performance [3]. Risk is the possibility of an event occurring that could result in losses for a business [4]. Risks are events that have negative impacts on the goals and strategies a company aims to achieve [5]. Identifying and measuring the possibility and consequences of risks in the operation of a company are fundamental tasks [6], [7]. Disruptions in information system technology directly or indirectly interfere with the business processes of an organization [8].

The Indonesian Red Cross Society (PMI) is a national association in Indonesia, legally recognized by Presidential Decree RIS Number 25 of 1950 and Presidential Decree RI Number 246 of 1963, operating in the fields of social welfare and humanitarian aid. The Indonesian Red Cross (PMI) has an information system to support its healthcare services. One of these information systems is the Clinic Management Information System (Smart Clinic), which is used to register patients from their arrival until they receive medication. In various situations, risks can lead to the destruction or loss of an organization [9]. In the process of using the PMI Main Clinic information system, no risk analysis has been conducted regarding the use of the Smart Clinic system, resulting in issues related to its usage [10]. Problems and risks often arise. If a risk occurs within an organization, it can lead to significant losses and hinder healthcare services [11].

ISO 31000 is a guide detailing the implementation of risk management through three components: framework, principles, and processes. This document provides the basis, principles, and processes that can serve as a basic structure

***Corresponding author: Wahyu Setiawan Basri (wsbasri@ui.ac.id)**
DOI: https://doi.org/10.47738/ijaim.v4i1.70

for efficient risk management within an organization [12]. This risk management framework is fully integrated with the strategic and operational policies and practices of the organization [13]. In efforts to control risks, ISO/IEC 27001 can be referenced. ISO/IEC 27001 is an international standard formulated for implementing, establishing, monitoring, operating, and maintaining Information Security Management Systems (ISMS) [14]. This standard serves as a broad reference for information security management, offering comprehensive guidance for managing information security within organizations [15]. ISO/IEC 27001 is not dependent on IT products, requires a risk-based management approach, and is designed to ensure that selected security controls can protect information assets from various risks [16].

The aim of this research is to analyze and identify the level of risk assessment in the information system at the PMI Main Clinic. Previous research has been conducted using ISO 31000:2018 in the field of education [17] and also in the field of technology [18], but has not yet utilized recommended handling procedures based on ISO/IEC 27001:2022.

2. Literature Review

Information systems (IS) play a pivotal role in modern healthcare organizations, enabling efficient delivery of patient services and management of clinical operations. With the increasing reliance on IS, the need for robust risk management practices becomes imperative to safeguard sensitive data, ensure uninterrupted operations, and mitigate potential threats [19].

Theoretical frameworks such as ISO 31000:2018 provide a systematic approach to risk management, offering guidelines for identifying, assessing, and mitigating risks within organizational contexts. ISO 31000 emphasizes a proactive and comprehensive approach, aligning well with the dynamic nature of healthcare environments where emerging threats necessitate continuous adaptation and response.

In conjunction with ISO 31000, the integration of ISO/IEC 27001:2022 control standards add further depth to the risk management framework proposed by the researchers. ISO/IEC 27001:2022 offers specific controls tailored to information security management systems, encompassing areas such as equipment maintenance, data backup, malware protection, and network security. By leveraging these standards, healthcare organizations can establish robust mechanisms to safeguard patient information, preserve data integrity, and ensure regulatory compliance.

Existing literature underscores the importance of proactive risk management strategies in healthcare settings, particularly in light of escalating cyber threats, regulatory complexities, and the increasing digitization of patient records. Studies by scholars such as Mehta et al. [20] have highlighted the vulnerabilities inherent in healthcare information systems and emphasized the need for multifaceted risk mitigation approaches.

Moreover, empirical research examining the implementation of ISO standards in healthcare organizations has demonstrated promising outcomes in terms of enhancing information security posture, fostering organizational resilience, and promoting a culture of risk-awareness among stakeholders.

In summary, the research conducted by the authors addresses a critical gap in healthcare risk management practices by proposing a comprehensive framework informed by ISO standards. By applying ISO 31000:2018 and ISO/IEC 27001:2022 control standards, the study offers practical insights for PMI Main Clinic and other healthcare organizations seeking to fortify their information systems against emerging threats and ensure the continuity of quality patient care.

3. Method

3.1. Data Collection Phase

Data collection was carried out to fulfill the required data through several methods. These methods encompassed a variety of approaches aimed at gathering comprehensive and accurate information. Among the strategies employed were surveys, interviews, observational studies, and document analysis. Each method was selected based on its appropriateness to the specific research objectives and the nature of the data sought. Surveys allowed for the collection of large amounts of data from a diverse range of participants, providing valuable insights into trends and patterns. Interviews provided the opportunity to delve deeper into the perspectives and experiences of individuals, offering rich

qualitative data. Observational studies enabled direct observation of phenomena in their natural settings, facilitating the exploration of behavior and interactions in real-time. Document analysis involved the systematic review and interpretation of written or recorded materials, offering valuable historical or contextual insights. By employing a combination of these methods, the data collection process aimed to capture a comprehensive understanding of the phenomenon under investigation.

3.1.1. Interviews

Interviews were conducted with the staff of the PMI Main Clinic, which encompassed administrative personnel and system managers at PMI, alongside the leaders of the PMI Main Clinic in their capacity as policy makers. Throughout this process, various operational and strategic aspects of the clinic were extensively discussed. The interviewing team gained valuable insights into how the clinic is run on a day-to-day basis, including the challenges faced and the strategies employed to address them. Moreover, the perspectives of the clinic leaders as policy makers provided a deeper understanding of the vision and strategic direction desired by PMI in providing healthcare services to the community. By broadening the scope of interviews to various levels of staff and management, this research aims to obtain a comprehensive overview of the various factors influencing the operational and strategic success of the PMI Main Clinic.

3.1.2. Observation

This stage entails direct observations through visits to the PMI Main Clinic to identify the existing assets and common challenges. These observations encompass in-depth research into various aspects, including infrastructure, human resources, and operational processes related to the healthcare services provided by PMI. Through these on-site visits, the team can gain a better understanding of the working environment and the prioritized needs to enhance efficiency and effectiveness in healthcare service delivery at the PMI Main Clinic.

3.1.3. Literature Review

The initial step in conducting this research involved a comprehensive literature review, which aimed to gather a wide array of scholarly sources including journals, books, and relevant readings. This thorough examination was specifically focused on the domain of information system risk management. The primary objective was to collect an extensive body of literature that could serve as foundational references and provide valuable insights for comparison throughout the writing process. Through this systematic review, a diverse range of perspectives and approaches within the field were synthesized, enabling a nuanced understanding of the subject matter and facilitating informed analysis and discussion in the subsequent research.

3.1.4. Questionnaire

Questionnaires were carefully administered to evaluate the risk level at the PMI Main Clinic, covering a broad spectrum of stakeholders including system users, developers, and policy makers. These questionnaires were meticulously distributed to ensure comprehensive feedback from each group, aiming to capture nuanced perspectives on potential risks and vulnerabilities within the clinic's operations. By involving various stakeholders, the assessment process sought to gather diverse insights and opinions, thereby enhancing the depth and accuracy of the risk evaluation conducted at the PMI Main Clinic.

3.1.5. Documentation

Documentation is a crucial aspect of any process or project, as it involves the meticulous collection and organization of information gleaned from existing documents or written records. Whether it's in the realm of business, academia, or research, documentation serves as a repository of knowledge, enabling stakeholders to access and understand pertinent details. Through thorough documentation practices, individuals can track progress, analyze historical data, and ensure compliance with regulations or standards. Moreover, comprehensive documentation enhances transparency and facilitates effective communication among team members, fostering collaboration and informed decision-making. Therefore, investing time and effort into proper documentation procedures is essential for promoting efficiency, accuracy, and accountability in various endeavors.

3.2. Problem Identification Phase

After obtaining data from the data collection phase, the next step in the process involved thorough analysis to identify any underlying problems and meticulously describe the issues associated with the implementation of information systems at the PMI Main Clinic. This analysis delved into various aspects such as system functionality, user experience, integration challenges, and potential technical constraints. Through this comprehensive examination, a detailed understanding of the existing issues was gained, enabling the formulation of effective strategies to address them. Additionally, the analysis provided valuable insights into areas requiring improvement or optimization within the information systems framework. This process served as a crucial foundation for devising tailored solutions and implementing enhancements to ensure the seamless operation and optimal performance of the information systems at the PMI Main Clinic.

3.3. Implementation of International Organization for Standardization (ISO) 31000:2018

This phase involved analyzing the risk management process at the PMI Main Clinic and was divided into five stages. The first stage encompassed data collection, wherein information pertaining to existing risks was gathered from various sources, including medical records, incident reports, and interviews with clinic staff. Subsequently, the collected data was analyzed to identify potential risk patterns and their potential impacts on clinic operations. Following this, the third stage involved risk assessment, wherein the identified risks were evaluated based on their severity and probability of occurrence. These assessment results were then utilized to design appropriate risk management strategies aimed at mitigating or controlling these risks. Finally, the fifth stage entailed the implementation of the designed risk management strategies, involving the application of corrective and preventive measures and continuous monitoring to ensure their effectiveness in managing risks at the PMI Main Clinic.

3.3.1. Communication and Consultation

Effective communication and consultation with stakeholders play a pivotal role in the comprehensive assessment of risks, as they provide diverse perspectives crucial for informed decision-making. In order to gain deeper insights into the practical implementation of risk management strategies, a series of observations and interviews were conducted with the Head of Administration. These interactions served as invaluable opportunities to delve into the nuances of risk identification, evaluation, and mitigation within the organizational framework. By engaging with key stakeholders and tapping into their expertise, a more robust understanding of potential risks and corresponding management strategies can be developed, thus enhancing the overall resilience and adaptability of the organization in the face of uncertainty.

3.3.2. Establishing Context

Establishing the context of risk management entails recognizing and defining boundaries that govern the risk management process. This involves considering various factors such as organizational objectives, the types of risks involved, the stakeholders affected, and the extent and depth of the risk management processes. By comprehensively understanding this context, organizations can better identify risks and plan appropriate strategies to manage them effectively.

3.3.3. Risk Assessment

Risk assessment at the PMI Main Clinic's information system was conducted through a comprehensive three-step process. The first step, risk identification, involved recognizing various assets within the system, as well as potential risks that could compromise its integrity or functionality. This phase also entailed assessing the potential impacts of these risks on the organization's operations and objectives. Following risk identification, the second step, risk analysis, categorized the identified risks based on their severity and likelihood of occurrence. This allowed for a deeper understanding of each risk's potential impact on the organization and helped prioritize them for mitigation efforts. Finally, in the third step, risk evaluation, the calculated risks were compared using predefined criteria, such as impact and likelihood, to determine their overall significance to the organization. This step facilitated informed decision-making regarding which risks required immediate attention and allocation of resources for mitigation strategies. By following this structured approach, the PMI Main Clinic was able to systematically identify, analyze, and evaluate risks within its information system, ultimately enhancing its resilience and security posture.

3.3.4. Risk Treatment

After conducting risk evaluations and providing recommendations for handling and prevention efforts, risk treatment was implemented in accordance with ISO/IEC 27001:2022 standards, which offer controls to mitigate risks. This risk treatment process involves concrete steps to identify, assess, and reduce identified risks within the system or organization. Furthermore, the implementation of these standards also encompasses the development and enforcement of appropriate security policies, as well as training for relevant staff, thereby enhancing awareness and skills in managing information security risks. Thus, these measures help establish a robust framework for safeguarding sensitive information and reducing the potential losses that could result from attacks or data breaches.

3.3.5. Monitoring and Review

Regular monitoring and review involving all stakeholders are essential aspects of effective risk management. By consistently assessing the current state of affairs and soliciting feedback from relevant parties, organizations can identify potential risks and address them proactively. Moreover, documenting the outcomes of these assessments and reviews ensures that valuable insights are preserved for future reference. This archival of data and insights serves as a foundation for refining and improving risk management strategies over time, enhancing the organization's ability to anticipate and mitigate potential threats. Thus, fostering a culture of ongoing monitoring, review, and documentation not only bolsters current risk management efforts but also lays the groundwork for continuous improvement and resilience in the face of evolving challenges.

4. Result and Discussion

The PMI Main Clinic has not effectively integrated the risk management information system, and the utilization of the information system is not adequately supported by established standard operating procedures. The management of information system risks is currently handled without clear procedures, relying solely on experience without specific risk mitigation guidelines. Therefore, the researchers aimed to assess the application of the ISO 31000 method in risk management at the PMI Main Clinic. The following section outlines the ISO 31000 stages:

4.1. Establishing Context

Context refers to all elements within the internal (internal context) and external (external context) environments in which the organization seeks to achieve its objectives. This context needs to influence the quality and, therefore, must be considered in the implementation of the risk management process. Some examples of internal context and their impacts on the risk management process that the organization will undertake include:

Table 1. Internal Context

No.	Internal Context	Influence on Risk Management
1.	Organizational Structure	Assignment of responsibilities, communication and collaboration, business continuity.
2.	Human Resources	Involvement and awareness of employees, information security training, security culture.
3.	Organizational Objectives	Alignment with business strategy, performance measurement, focus on information value.

Meanwhile, some examples of external context and their influences on the risk management process that the organization will undertake include:

Table 2. External Context

No	External Context	Impact on risk management
1.	Legal Regulations and Rules	Determining the legal framework and compliance requirements to be followed by the organization. Introducing information security requirements that must be complied with. Identifying sanctions or legal consequences related to information security breaches.

		Encouraging organizations to adopt good information security practices.
2.	Stakeholders	Determining the expectations and needs of stakeholders regarding information security. Influencing the setting of risk management objectives and priorities. Ensuring compliance with ethical standards and social responsibilities. Encouraging transparency and effective communication about risk management with stakeholders.
3.	Cloud Service Providers	Providing or managing technology infrastructure that may have specific security risks. Providing cloud security services that can influence organizational information security policies. Having security policies and practices to be considered in risk management. Establishing requirements and limitations related to information security at the level of cloud service provision.
4.	Relationship with Business Partners	Risk assessment of third-party involvement and business partner engagement in risk management. Drafting strong information security agreements with business partners.

4.2. Risk Assessment

The risk assessment stage at the PMI Main Clinic consists of three steps: risk identification, risk analysis, and risk evaluation to determine the potential threats to the assets present at the PMI Main Clinic.

Table 3. Risk Identification

No	Risk	Impact
1.	Server Down	The system cannot be accessed and disrupts service processes.
2.	Hardware Failure	Reduces company assets, hardware replacement, and disrupts service processes.
3.	Data Loss	Loss of medical record data and loss of important data.
4.	Web service hang/error	The system cannot be accessed, may lose data, and disrupts diagnosis processes.
5.	Virus Attacks on Systems	Data cannot be read and data loss.
6.	System Shutdown Suddenly	Hardware damage, data loss, and productivity disruption.
7.	Network Disconnection	The system cannot be accessed, disrupts service processes, and communication interruptions.
8.	Data Input Errors	Patient data input errors and operational disruptions.
9.	Misuse of Access Rights	Data loss and serious security breaches.
10.	Unscheduled Maintenance	System or hardware damage, operational disruptions, and data loss.
11.	Device/Data Theft	Loss of assets and loss of critical data.
12.	Former Employees Still Have Access to the System	Data security risks, data deletion risks, and data loss.
13.	Leakage of Company Information Data	Loss of critical data.
14.	Power Outage	The system cannot be accessed and medical equipment cannot be used.
15.	Non-Functioning Generator	Disrupts processes in the organization.
16.	Outdated Technology	Disrupts service processes and slows down the system.
17.	Fire Alarm Malfunction	Endangers in case of fire.
18.	CCTV Malfunctioning	Disrupted monitoring and reduced security levels.
19.	Volcanic Eruption	Damage to facilities and infrastructure and disrupted healthcare service processes.

 ISSN 2776-8007

20.	Fire	The system cannot be accessed and disrupts service processes.
21.	Earthquake	Reduces company assets, hardware replacement, and disrupts service processes.
22.	Lightning	Loss of medical record data and loss of important data.

The next step is to determine indicators to assess the previously identified threats. The existence of risk probability indicators and risk impact values allows for measuring the existing level of risk by listing these probability and risk impact values.

Table 4. Probability Values

Criteria	Description	Value	Event Frequency
Certain	Certain Risk	5	< 7 months
Likely	Likely Risk	4	7 - 12 months
Possible	Possible Risk	3	1 - 3 years
Unlike	Unlikely Risk	2	3 - 5 years
Rare	Rarely Occurring Risk	1	> 5 years

The following table shows the likelihood (likelihood) and impact values to measure the level of existing risks. The risk assessment frequency is divided into 5 criteria, ranging from certain with a frequency value of 5, indicating a definite risk occurrence (<7 months), to rare with a frequency value of 1, indicating an almost never occurrence (>5 years). For risk impact assessment, please refer to Table 5.

Table 5. Risk Impact

Criteria	Description	Value
Major	The occurring risks severely disrupt company activities and cause the entire business operations to come to a halt.	5
High	The occurring risks begin to disrupt company activities and interfere with the operation of applications, leading to impediments.	4
Moderate	The occurring risks start to disrupt some company activities and hinder the smooth operation of applications.	3
Minor	The occurring risks slightly disrupt company activities and mildly impede the operation of applications.	2
Insignificant	The occurring risks do not disrupt company activities and the operation of applications.	1

To assess risk impact, impact values are divided into five criteria, each with different risk levels. Risk impact assessment consists of five criteria: major, high, moderate, minor, and insignificant, with frequency values from 5 to 1. Based on risk identification, the results of probability and impact assessment can be seen in Table 6 below:

Table 6. Risk Analysis

Risk	Frequency	Impact
Server Down	4	4
Hardware Damage	4	1
Data Loss	1	4
Web service hang/error	4	4
Virus Attack on the system	1	4
Sudden system shutdown	2	4
Network disconnection	5	4
Data input errors	5	2

Misuse of access rights	3	2
Unscheduled maintenance	3	2
Device/data theft	1	3
Former employees still have access to the system	1	1
Company data information leakage	1	1
Power outage	5	5
Non-functional generator	1	5
Outdated technology	1	1
Firefighting equipment malfunction	1	1
CCTV malfunction	1	1
Volcanic eruption	1	4
Fire	1	5
Earthquake	1	5
Lightning	1	4

The next stage is the risk evaluation stage, which compares the results of the risks identified in the previous analysis stage against risk parameters. The identified risk levels can be seen in the table below:

Table 7. Risk Evaluation

Risk	**Frequency**	**Impact**	**Risk Levels**
Server downtime	4	4	Very High
Hardware damage	4	1	Moderate
Data loss	1	4	Moderate
Web service hang/error	4	4	Very High
Risk	**Frequency**	**Impact**	**Risk Levels**
Virus attacks on the system	1	4	Moderate
Sudden system failure	2	4	High
Network disconnection	5	4	Very High
Data input errors	5	2	High
Misuse of access rights	3	2	Moderate
Unscheduled maintenance	3	2	Moderate
Device/data theft	1	3	Low
Former employees still have access to the system	1	1	Low
Company data leakage	1	1	Low
Power outage	5	5	Very High
Non-functional generator	1	5	Moderate
Outdated technology	1	1	Low
Fire extinguishing equipment malfunction	1	1	Low
CCTV malfunction	1	1	Low
Volcanic eruption	1	4	Moderate
Fire	1	5	Moderate
Earthquake	1	5	Moderate
Lightning	1	4	Moderate

4.3. Risk Control

In the risk treatment phase, risk treatment actions will be applied to the identified and evaluated risks during the risk assessment stage. The aim of these risk treatment actions is to reduce the likelihood of these risks occurring. Risk treatment can be arranged based on the identified risk levels, ranging from very high, high, moderate, to low risks, following the guidelines provided by ISO 27001:2022:

Table 8. Risk Control

Risks	Risk Levels	Risk Treatment (In accordance with ISO 27001:2022)
Server downtime	Very High	It is important to maintain equipment properly to ensure the availability, integrity, and confidentiality of information (7.13). Additionally, regular maintenance and testing of backup copies of information, software, and systems should be conducted according to agreed backup policies (8.13). Steps and procedures must be implemented to ensure the secure management of software installations on operational systems (8.19).
Web service hang/error	Very High	Established procedures need to be followed in the process of acquiring, using, managing, and exiting from cloud services in line with organizational information security requirements (5.23). Network, system, and application monitoring for anomalous behavior should be performed, and appropriate steps should be taken to assess potential information security incidents (8.16). Implementation of procedures and actions is required to ensure the secure management of software installations on operational systems (8.19). Management of access to external websites should also be carefully conducted to reduce exposure to harmful content (8.23).
Network disconnection	Very High	Network security must be ensured by maintaining and controlling network controls and network devices to protect information within systems and applications (8.20). Network services also need to be managed by identifying, implementing, and monitoring security mechanisms, service levels, and appropriate service requirements (8.21). To maintain security, network segregation is necessary by separating information service groups, users, and information systems within the organizational structure (8.22).
Power outage	Very High	Secure system engineering principles need to be defined, documented, maintained, and applied at every stage of information system development (8.27).
System sudden shutdown	High	Implementation of procedures and measures is required to maintain software installations on operational systems securely (8.19). Efforts to protect against malware should be implemented, supported by adequate user awareness (8.7). Regular maintenance and testing of backup copies of information, software, and systems should be performed according to agreed backup policies (8.13).
Data input error	High	Organizational personnel and relevant parties need to receive appropriate information security awareness, education, and training, as well as periodic updates on organizational information security policies, and policies and specific procedures relevant to their job duties (6.3). Disciplinary processes need to be formally defined and communicated to take action against personnel and other relevant parties who violate information security policies (6.4).
Hardware damage	Moderate	Equipment needs to be securely placed and protected (7.8). To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).

Data loss	Moderate	Regular maintenance and testing of backup copies of information, software, and systems should be performed according to agreed backup policies (8.13).
Virus attack on the system	Moderate	Efforts to protect against malware should be implemented, supported by adequate user awareness (8.7). Regular maintenance and testing of backup copies of information, software, and systems should be performed according to agreed backup policies (8.13).
Misuse of access rights	Moderate	Rules for controlling physical and logical access to information and other related assets need to be defined and implemented in line with business and information security requirements (5.15). Organizational personnel and relevant parties need to receive appropriate information security awareness, education, and training, including periodic updates on organizational information security policies, as well as policies and specific procedures relevant to their job duties (6.3). Access to information and other related assets should be restricted according to specific access control policies (8.3).

Risk	**Risk Levels**	**Perlakuan Risiko (Sesuai ISO 27001:2022)**
Unscheduled maintenance	Moderate	To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).
Non-functional generator	Moderate	To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).
Volcanic eruption	Moderate	Design and implementation of protection against physical and environmental threats, including natural disasters and other intentional or unintentional physical threats to infrastructure (7.5), are necessary. Regular maintenance and testing of backup copies of information, software, and systems should be conducted in accordance with approved backup policy topics (8.13).
Fire	Moderate	Design and implementation of protection against physical and environmental threats, including natural disasters and other intentional or unintentional physical threats to infrastructure (7.5), are necessary. Regular maintenance and testing of backup copies of information, software, and systems should be conducted in accordance with approved backup policy topics (8.13).
Earthquake	Moderate	Design and implementation of protection against physical and environmental threats, including natural disasters and other intentional or unintentional physical threats to infrastructure (7.5), are necessary. Regular maintenance and testing of backup copies of information, software, and systems should be conducted in accordance with approved backup policy topics (8.13).
Lightning	Moderate	Design and implementation of protection against physical and environmental threats, including natural disasters and other intentional or unintentional physical threats to infrastructure (7.5), are necessary. Regular maintenance and testing of backup copies of information, software, and systems should be conducted in accordance with approved backup policy topics (8.13).
Theft of devices/data	Low	Security perimeter controls need to be established and implemented to maintain the security of areas containing information and other related assets (7.1). Secure areas must be protected with appropriate entry controls and access points (7.2). The design and implementation of physical security controls for offices, rooms, and facilities must also be applied (7.3).
Former employees still have access to the system	Low	Access to information and other related assets must be restricted according to specific policies related to access control topics (8.3).

Leakage of company information data	Low	Rules for controlling physical and logical access to information and other related assets must be explained and implemented in accordance with business requirements and information security (5.15). Access to information and other related assets must be restricted according to specific policies on access control topics (8.3).
Outdated technology	Low	To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).
Non-functional fire extinguishing equipment	Low	To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).
CCTV malfunction	Low	To ensure the availability, integrity, and confidentiality of information, equipment must receive appropriate maintenance (7.13).

4.4. Monitoring and Review

In this phase, activities involve providing suggestions and criticisms to PMI Adhyaksa with the aim of improving the handling of potential risks. Through scheduled monitoring and review activities, emerging obstacles are identified, and efforts are made to reduce the likelihood of risks. Monitoring and review are carried out regularly through meetings discussing the implementation of information systems, focusing on obstacles or risks that may hinder the business processes of PMI Adhyaksa. This discussion aims not only to address obstacles but also to design preventive measures to minimize potential risks.

5. Conclusion

The results of risk management analysis at the PMI Main Clinic using the ISO 31000:2018 method can be summarized as follows: Out of 22 identified risks, 4 were classified as Very High, 2 as High, 10 as Moderate, and 6 as Low. Common potential threats include server downtime, web service errors, network disconnections, and power outages. Specific actions are required to address these risks. The analysis and assessment of risks have assisted the PMI Main Clinic in minimizing risks and implementing necessary improvements. Recommendations for controls, referring to ISO/IEC 27001:2022, include Equipment maintenance, Information backup, Protection against malware, Installation of software on operational systems, Monitoring activities, Web filtering, Network security, Security of network services, Segregation of networks, and Secure system architecture and engineering principles. These control recommendations are outlined in the form of standard operating procedures for risk management at the PMI Main Clinic.

6. Declarations

6.1. Author Contributions

Conceptualization: W.S.B. and A.L.A.; Methodology: A.L.A.; Software: W.S.B.; Validation: W.S.B., A.L.A.; Formal Analysis: W.S.B., A.L.A.; Investigation: W.S.B.; Resources: A.L.A.; Data Curation: A.L.A.; Writing Original Draft Preparation: W.S.B. and A.L.A.; Writing Review and Editing: A.L.A. and W.S.B.; Visualization: W.S.B.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The author would like to express gratitude to the PMI for their support in this research.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Monica, didik Kurniawan, dan R. Prabowo, "Analisis Manajemen Risiko Sistem Informasi Pengelolaaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," *J. Komputasi*, vol. 8, no. 1, pp. 83–90, 2020, doi: 10.23960/komputasi.v8i1.2351.

[2] D. Anjeli, S. Tita Faulina, dan A. Fakih, "Sistem Informasi Perpustakaan Sekolah Dasar Negeri 49 OKU Menggunakan Embarcadero XE2 Berbasis Client Server," *J. Inform. dan Komput., vol.* 13, no. 2, pp. 57–66, 2022.

[3] F. M. Hutabarat dan A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[4] J. M.Kom, "Sistem Informasi Penerimaan Siswa Baru Berbasis Web Di Sekolah Menengah Pertama Negeri 43 Palembang," *J. Digit. Teknol. Inf.*, vol. 1, no. 2, pp. 98, 2020, doi: 10.32502/digital.v1i2.2370.

[5] G. Lantang, A. Cahyono, dan M. Sitokdana, "ANALISIS RISIKO TEKNOLOGI INFORMASI PADA APLIKASI SAP DI PT SERASI AUTORAYA MENGGUNAKAN ISO 31000," *Sebatik*, vol. 23, pp. 36–43, Jun 2019, doi: 10.46984/sebatik.v23i1.441.

[6] P. Kanantyo dan F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 1896–1908, 2021, doi: 10.35957/jatisi.v8i4.1082.

[7] C. Sianipar, "Analisis Manajemen Risiko Dan Kontrol Pada Seksi Sistem Informasi Berdasarkan Iso 31000 Studi Kasus : Pt . Nusantara Regas," vol. 9, no. 2, pp. 610–618, 2022.

[8] D. I. Izatri, N. I. Rohmah, dan R. S. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, pp. 50, 2020, doi: 10.30865/jurikom.v7i1.1756.

[9] N. Noviyanti, A. Aristoteles, Y. Heningtyas, dan T. Tristiyanto, "Analisis Manajemen Risiko Sistem Informasi Kkn Universitas Lampung Menggunakanmetode Nist 800- 30," *J. komputasi*, vol. 6, no. 2, pp. 1–10, 2018.

[10] N. Matondang, I. N. Isnainiyah, dan A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[11] I. P. S. Arta dkk., Manajemen Risiko, Tinjauan Teori Dan Praktis. 2021.

[12] D. L. Ramadhan, R. Febriansyah, dan R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, pp. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

[13] L. E. Hutagalung, "Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rumah Sakit Xyz Menggunakan Iso 31000," *TeIKa*, vol. 12, no. 01, pp. 23–33, 2022, doi: 10.36342/teika.v12i01.2820.

[14] I. Setiawan, A. R. Sekarini, R. Waluyo, dan F. N. Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 2, pp. 389–396, 2021, doi: 10.30812/matrik.v20i2.1093.

[15] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 2, pp. 764–773, 2021, doi: 10.35957/jatisi.v8i2.789.

[16] D. S. Valena, rizky prabowo, anie rose irawati, dan aristoteles aristoteles, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode Nist Sp 800-30," *J. Komputasi*, vol. 7, no. 1, pp. 1–10, 2019, doi: 10.23960/komputasi.v7i1.2053.

[17] R. R. Afrininda, "Analisis Manajemen Risiko Aplikasi Ujian Online dengan Metode OCTAVE Allegro pada lembaga pendidikan," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 6, no. 2, pp. 62–73, 2021, doi: 10.32528/justindo.v6i2.4546.

[18] S. P. Zagoto dan M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Di Organisasi Xyz Cabang Salatiga

Menggunakan Iso 31000," *J. Mnemon.*, vol. 4, no. 1, pp. 1–9, 2021.

[19] O. Budak and M. Filiz, "The moderating role of work experience in the effect of ethical culture on whistleblowing in healthcare professionals and the effect of Organizational Trust on whistleblowing," *Enfermería Clínica (English Edition)*, vol. 1, no. 1, pp. 1–12, Apr. 2024. doi:10.1016/j.enfcle.2024.04.003

[20] Y. Mehta, C. Mehta, and A. Chandrasekaran, "Aviptadil: A multifaceted approach to mitigating hypoxemia in acute respiratory distress syndrome," *Respiratory Medicine Case Reports*, vol. 48, no. 1, pp. 101992–101999, 2024. doi:10.1016/j.rmcr.2024.101992