Journal of Information Systems and Informatics

Vol. 5, No. 2, June 2023 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v5i2.468 Published By DRPM-UBD

Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework

Niken Lusia Putri [1], Agustinus Fritz Wijaya [2]

[1,2] Faculty of Information Technology, Satya Wacana Christian University, Salatiga, Indonesia
[1] 682019166@student.uksw.edu, [2] agustinus.wijaya@uksw.edu

Abstract

As information technology becomes increasingly integrated into daily business processes within educational institutions in Indonesia, the need to address potential risks associated with this integration has become crucial. This research focuses on analyzing information technology risk management in Indonesian educational institutions using the ISO 31000 framework. The study aims to minimize the occurrence and impact of various information technology risks that can disrupt organizational processes. Through a comprehensive examination encompassing risk assessment, analysis, evaluation, and treatment, this research provides valuable insights into identifying potential risks within educational institutions. Furthermore, the findings serve as a reference for formulating risk management policies, enabling institutions to proactively mitigate the possibility of information technology risks and their future impact. By adopting the ISO 31000 framework, educational institutions can enhance their efficiency, effectiveness, and accessibility while safeguarding against potential disruptions.

Keywords: information technology, risk management, ISO 31000, educational institution

1. INTRODUCTION

In the era of globalization, information technology is rapidly advancing, impacting various institutions in Indonesia, including health, legal, social, economic, and educational institutions. The integration of information technology is essential, particularly in educational institutions, where it serves as a vital support for daily business activities, improving academic services and striving towards institutional goals. Furthermore, information technology plays a crucial role in enabling educational institutions to compete in the current era of globalization [1]. Consequently, the implementation of information technology is imperative for diverse educational institutions in Indonesia.

Presently, one particular educational institution in Indonesia has successfully integrated information technology into its daily business processes. An example of this integration is the utilization of SIAHDU (Integrated School Information System) for processing administrative data and information related to students. SIAHDU, a custom-built application system, manages student administrative data such as violation records, biographical information, grades, attendance, and report cards within the institution. Accessible to teachers, school staff, students, and parents, SIAHDU is complemented by additional application systems, such as SIKADU (Integrated Academic System) and SISMINDO (Integrated Administrative System). While leveraging information technology offers significant benefits, it is essential to acknowledge the potential risks that can affect the optimal performance of these application systems [2]. Such risks, stemming from various factors, can disrupt the ongoing business processes or activities within educational institutions. Additionally, the effective execution of an organization's business processes necessitates skilled human resources and robust systems and infrastructure [3]. Therefore, conducting an analysis of information technology risk management at these educational institutions becomes imperative.

Risk management encompasses a set of policies and procedures owned by organizations, enabling them to effectively manage, monitor, and control risks within their operations [4]. By implementing risk management practices, organizations can protect themselves from potential risks and mitigate their impact on business processes, ultimately facilitating the achievement of organizational goals [5]. Consequently, risk management garners significant interest within organizations as it aids in minimizing potential losses caused by unforeseen risks.

The integration of information technology into educational institutions has witnessed rapid growth in recent years, including within Indonesia. This integration has yielded numerous advantages, such as enhanced efficiency, effectiveness, and information accessibility. However, it has also introduced a range of information technology risks capable of disrupting the daily business processes of educational institutions. These risks encompass cyber threats, data breaches, system failures, and human errors. Given the pivotal role of information technology in educational institutions, it is crucial to ensure the effective management of associated risks. Accordingly, this research proposes the utilization of the ISO 31000 framework as a comprehensive guide for analyzing information technology risk management in Indonesian educational institutions. Widely recognized and accepted as a standard for risk management, this framework offers a structured and systematic approach to risk identification, assessment, and treatment. The research endeavors to identify potential information technology risks present in Indonesian educational institutions, assess their likelihood and potential impact, and develop a risk treatment plan aimed at minimizing both the occurrence and impact of these risks. The findings of this research will offer valuable insights to educational institutions in Indonesia, aiding in the identification of risks within their organizations and the formulation of policies to effectively address them. Ultimately, this research aims to reduce the likelihood and impact of information technology risks, ensuring seamless operations within Indonesian educational institutions.

This research conducted a thorough analysis of information technology risk management within an educational institution in Indonesia, employing the ISO 31000 framework. The selection of the ISO 31000 framework was motivated by its comprehensive nature, encompassing risk identification, assessment, and management. It offers organizations a structured and efficient risk management process, aligning with their needs. Notably, ISO 31000 adopts a risk-based approach, empowering organizations to determine appropriate actions for risk handling and reduction through systematic risk identification and evaluation. Consequently, organizations can prioritize risk mitigation according to the level of risk involved. Another advantage of the ISO 31000 framework is its applicability across diverse sectors and organizational sizes, rendering it well-suited for educational institutions.

The research yielded valuable insights into risk assessment, risk analysis, risk evaluation, and risk treatment pertaining to various information technology risks within the educational institution under study. The study outcomes are expected to assist educational institutions in identifying potential risks within their organizational context. Furthermore, the findings can serve as a valuable reference for formulating policies concerning risk treatment, empowering organizations to effectively mitigate the occurrence and impact of information technology risks both presently and in the future.

2. METHODS

The research methodology employed in the analysis of information technology risk management aligns with the stages adapted from the ISO 31000:2019 framework [6]. Data and information for this study were collected through qualitative descriptions obtained via interviews with internal sources within an Indonesian educational institution. This approach enabled the acquisition of firsthand insights and statements pertaining to the specific challenges encountered within the institution [7]. The research methodology stages are illustrated in Figure 1.

1. Communication and Consultation, the purpose of this stage is to help stakeholders enhance their understanding of the risks involved and the importance of identifying suitable measures to manage those risks.
2. Scope, Context, and Criteria, this stage aims to adjust the risk management process, enabling efficient risk assessment and appropriate risk treatment by defining scope of the process and comprehending the internal and external context.

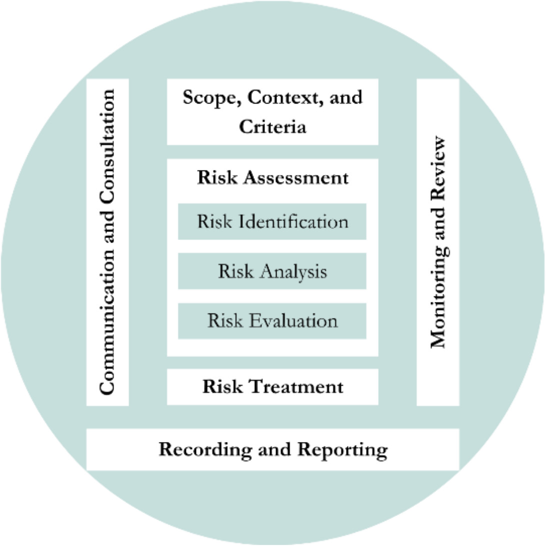

Figure 1. Risk Management – Process [6]

3. Risk assessment, the stage of determining information technology risks that may occur in an educational institution in Indonesia so that it can influence the institution in achieving its goals. In this stage there are three processes, namely risk identification, risk analysis, and risk evaluation. Risk identification is a process to find, recognize, and define information technology risks that may occur in the institution. In risk identification there are several processes, such as identification of assets, possible risks, and the impact of risks. Meanwhile, risk analysis is a process that aims to understand information technology risks in these educational institutions more deeply, such as understanding the nature and characteristics of risks that are described using predetermined levels. Then is the process of evaluating the level of each information technology risk at the institution based on predetermined criteria. The risk evaluation process aims to support the decision-making process.
4. Risk treatment, this stage aims to select and select alternative information technology risk mitigation proposals at these educational institutions based on the results of the risk evaluation. It is hoped that the risk mitigation proposals provided by researchers can minimize or even eliminate the impact and the possibility of risk occurring if the proposal is applied to these educational institutions.
5. Monitoring and Review, the objective of this stage is to guarantee and enhance the quality and efficiency of process design, implementation, and results. It is necessary to include regular monitoring and periodic review of risk management process with clearly assigned responsibilities.
6. Recording and Reporting, the stage for documenting and reporting the results of risk management process through appropriate mechanism.

In addition, one of the methods used in this research is case study research. This method is a research method that focuses attention on a case by using individuals or groups as research material [8]. This method can be used to extract deeper data on the object being studied so that it can answer the problems that are currently happening at one of the educational institutions in Indonesia.

3. RESULTS AND DISCUSSION

3.1. Risk Assessment

In accordance with the ISO 31000 framework, the analysis of information technology risk management in an Indonesian educational institution followed a structured methodology. The initial stage, as per the framework, involved information technology risk assessment. This stage encompassed three fundamental processes: risk identification, risk analysis, and risk evaluation. During the risk identification process, potential information technology risks within the educational institution were systematically identified and documented. This involved a comprehensive examination of the institution's technological infrastructure, processes, and potential vulnerabilities.

Subsequently, the risk analysis process was conducted, aiming to assess the likelihood and potential impact of identified risks. Through careful examination and analysis of the identified risks, their probability of occurrence and potential consequences were evaluated. This step facilitated a deeper understanding of the risks' significance and provided a basis for subsequent risk management actions. Following risk analysis, the risk evaluation process was undertaken. This stage involved determining the priority and significance of each identified risk by considering factors such as potential impacts on the institution's business processes, resources, and stakeholders. By evaluating risks in a systematic and objective manner, the institution could effectively allocate resources and prioritize risk treatment strategies.

These three processes—risk identification, risk analysis, and risk evaluation—comprise the initial stage of information technology risk management analysis, as outlined by the ISO 31000 framework. These stages provided a structured approach to comprehensively assess and evaluate potential risks within the educational institution's information technology landscape.

3.1.1. Risk Identification

The risk assessment stage commences with the first vital process of risk identification, which involves three distinct components: the identification of assets, identification of potential risks, and identification of the impact associated with these risks. The first aspect of risk identification focuses on identifying the assets within the educational institution's information technology landscape. This entails recognizing and documenting the valuable resources, systems, data, and infrastructure that are susceptible to risks. By understanding the organization's assets, a comprehensive evaluation of potential risks can be conducted.

Subsequently, the second facet of risk identification entails identifying the diverse array of potential risks that could impact the institution's information technology environment. This involves a meticulous examination of various threat sources, vulnerabilities, and potential disruptions that could compromise the confidentiality, integrity, and availability of the institution's IT assets. By comprehensively identifying potential risks, the institution gains a comprehensive understanding of the landscape it faces. Furthermore, the third component of risk identification involves assessing the impact that these identified risks may have on the educational institution. This entails evaluating the potential consequences, both tangible and intangible, that could result from the occurrence of these risks. By considering factors such as financial losses, reputational damage, operational disruptions, and regulatory non-compliance, the institution gains insights into the potential severity and magnitude of the identified risks. Through this meticulous process of risk identification, encompassing the identification of assets, potential risks, and the impact of these risks, the educational institution establishes a solid foundation for effective risk management and mitigation strategies.

1) Asset Identification

The initial step of the risk identification process involves identifying the information technology (IT) assets within an Indonesian educational institution, accomplished through interviews conducted with informants from the institution. This process entails identifying the various data, software, and hardware components present within the institution's IT infrastructure. For a comprehensive understanding, Table 1 provides specific details regarding the IT assets found within the educational institution in Indonesia.

Table 1. Asset Identification

Technology Components	Educational Institution Assets
Data	Student Personal Data
	Student Violation Point Data
	Student Attendance Data
	Student Grade Data
	Student report card data
	Achievement Data
	Personnel Data
Software	SIAHDU (Integrated School Information System)
	SIKADU (Integrated Academic System)

	SISMINDO (Integrated Administration System)
hardware	Web Servers
	Application Servers
	Database Servers
	Internet Network
	Personal Computers (PCs)
	Laptops

Through the interview process, these crucial information technology assets have been identified and documented. This comprehensive inventory of assets provides a solid foundation for the subsequent stages of risk assessment and management within the educational institution.

2) Identification of Possible Risks

Following the process of identifying information technology (IT) assets, the subsequent step involves the identification of potential IT risks within an educational institution in Indonesia. These risks are classified and grouped based on various factors, including natural and environmental factors, human factors, as well as systems and infrastructure. Table 2 provides an overview of the possible information technology risks present in these institutions.

Table 2. Identification of Possible Risks

Factor	**ID**	**Possible Risks**
Nature and Environment	R01	Fire
	R02	Strong winds
	R03	Lightning
	R04	Earthquake
Man	R05	Lack of human resources in the information technology section in quality and quantity
	R06	Unscheduled system maintenance process
	R07	Logical attacks (hacking and malware)
	R08	New information technology staff don't understand how the system works yet
	R09	Admin negligence in the process of updating data and information
	R10	Information accessed by unauthorized parties
Systems and Infrastructure	R11	Hardware damage
	R12	Software failure
	R13	Data backup failure
	R14	Unstable internet network

	R15	Server down
	R16	Power outage

By categorizing the possible IT risks according to these factors, educational institutions can gain a clearer understanding of the specific risks they face. This knowledge empowers them to develop effective risk management strategies tailored to mitigate these identified risks.

3) Risk Impact Identification

The concluding phase of the risk identification process entails the identification of the potential impacts associated with each information technology risk. This crucial step involves assessing and documenting the effects that every possible risk may have on an educational institution in Indonesia. Table 3 provides an overview of the impacts that information technology risks can pose to these institutions.

Table 3. Risk Impact Identification

ID	Possible Risks	Impact
R01	Fire	Infrastructure damage and hinder the organization's business processes.
R02	Strong winds	Infrastructure damage and hinder the organization's business processes.
R03	Lightning	Infrastructure damage and hinder the organization's business processes.
R04	Earthquake	Infrastructure damage and hinder the organization's business processes.
R05	Lack of human resources in the information technology section in quality and quantity	Teachers and staff have to work concurrently as administrators of information technology so that there are difficulties in the division of labor.
R06	Unscheduled system maintenance process	If there is damage to the application system, the damage cannot be detected so that it can interfere with the performance of the application system.
R07	Logical attacks (hacking and malware)	Data and information are manipulated, stolen, and accessed by unauthorized parties. malware virus so that the organization's business processes can be disrupted

R08	New information technology staff don't understand how the system works yet	Difficulty in operating the system
R09	Admin negligence in the process of updating data and information	Data and information are invalid and do not match the facts. Reducing the level of organizational integrity.
R10	Data and information accessed by unauthorized parties	Organizational data and information can be misused.
R11	Hardware damage	Hardware cannot function properly. The application system cannot be accessed. Organizational business processes can be disrupted because a new hardware replacement is required.
R12	Software failure	May cause data loss.
R13	Data backup failure	There is no backup data in case the organization experiences data loss.
R14	Unstable internet network	Difficulty in accessing the application system.
R15	Server down	Database and software cannot be accessed.
R16	Power outage	All hardware cannot be used. Software cannot be accessed. Organizational business processes are hampered.

By comprehensively identifying the potential impacts of information technology risks, educational institutions can better understand the consequences these risks may have on their overall operations, financial standing, reputation, compliance obligations, and student services. This knowledge is essential for devising appropriate risk management strategies to mitigate the potential adverse effects and ensure the smooth functioning of the institution.

3.1.2. Risk Analysis

The subsequent stage in the risk assessment process is risk analysis. During this phase, the identified risks are evaluated by utilizing the likelihood criteria table and the impact criteria table. The likelihood criteria table serves as a reference to assess the probability of information technology risks occurring within a specified timeframe in an educational institution in Indonesia. Table 4 presents the five criteria used in the likelihood criteria table.

Table 4. Likelihood criteria

Likelihood		Description	Frequency of Events
Mark	**Criteria**		
1	Rare	This risk almost never occurs	> 2 years
2	Unlikely	Such risks are rare	1-2 years
3	Possible	These risks sometimes occur	7-12 months
4	Likely	This risk occurs frequently	4-6 months
5	certain	The risk is bound to happen	1-3 months

In addition, an impact criteria table is utilized as a reference for evaluating the magnitude of impact that each potential information technology risk may have on an educational institution in Indonesia within a specified timeframe. Table 5 delineates the five impact criteria, ranging from no effect to the highest impact that significantly affects the organization.

Table 5. Impact Criteria

Impact		Information
Mark	**Criteria**	
1	Insignificant	This risk does not interfere with the business processes running in the organization
2	Minor	This risk slightly hampers business processes but does not interfere with the main activities of the organization
3	Moderate	This risk hampers some of the business processes that run in the organization
4	majors	This risk disrupts almost all business processes that run in the organization
5	Catastrophic	This risk disrupts all business processes running in the organization so that the organization's activities stop

By utilizing these impact criteria, educational institutions can assess and categorize the potential impacts associated with each identified information technology risk. This assessment enables organizations to prioritize their risk management efforts and allocate resources, accordingly, ensuring a focused approach to mitigating risks that pose the greatest impact on their operations and objectives. The subsequent step involves evaluating each potential information technology risk present within an educational institution in Indonesia by assigning predetermined probability and impact values. A comprehensive assessment of the likelihood and impact of each possible information technology risk within the institution is provided in Table 6.

Table 6. Assessment of Likelihood and Impact on Possible Risks

ID	Possible Risks	Likelihood	Impact
R01	Fire	1	3
R02	Strong winds	3	4
R03	Lightning	4	5
R04	Earthquake	1	2
R05	Lack of human resources in the information technology section in quality and quantity	2	1
R06	Unscheduled system maintenance process	1	1
R07	Logical attacks (hacking and malware)	1	3
R08	New information technology staff don't understand how the system works yet	3	2
R09	Admin negligence in the process of updating data and information	5	5
R10	Information accessed by unauthorized parties	1	3
R11	Hardware damage	3	5
R12	Software failure	1	2
R13	Data backup failure	1	1
R14	Unstable internet network	2	3
R15	Server down	2	3
R16	Power outage	4	5

By utilizing the predetermined criteria for likelihood and impact, the assessment provides a detailed overview of the estimated likelihood and potential impact for each information technology risk within the educational institution. This analysis enables organizations to prioritize and focus their risk management efforts on risks that have higher probability and greater potential impact, ensuring a more targeted and effective risk mitigation strategy.

3.1.3. Risk Evaluation

The last stage in the risk assessment process is risk evaluation. At this stage, the identified possible information technology risks in an educational institution in Indonesia, along with the assigned likelihood and impact values from the previous process, are integrated into the risk evaluation matrix. The risk evaluation matrix serves as a tool to determine the risk level by categorizing it into three levels: low, medium, and high. The mapping of risk levels based on likelihood and impact values can be observed in Table 7.

Table 7. Risk Evaluation Matrix

Likelihood	**Certain**	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
Impact			**1**	**2**	**3**	**4**	**5**
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**

Each potential information technology risk within the educational institution will be incorporated into the risk evaluation matrix, aligning with the mapping provided in Table 7, considering the likelihood and impact values determined in the preceding process. Below is the risk evaluation matrix, adjusted to reflect the likelihood and impact values.

Table 8. Risk Evaluation Matrix Based on Likelihood and Impact

Likelihood	**Certain**	5					R09
	Likely	4					R03 R16
	Possible	3		R08		R02	R11
	Unlikely	2	R05		R14 R15		
	Rare	1	R06 R13	R04 R12	R01 R07 R10		
Impact			**1**	**2**	**3**	**4**	**5**
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**

Upon incorporating all possible information technology risks within the institution, considering their likelihood and impact values, the 16 aforementioned risks are categorized into three distinct risk levels: low, medium, and high levels.

Table 9. Risk Level of Possible Risk

ID	Possible Risks	Risk Level
R01	Fire	Low
R04	Earthquake	Low
R05	Lack of human resources in the information technology section in quality and quantity	Low
R06	Unscheduled system maintenance process	Low
R07	Logical attacks (hacking and malware)	Low
R10	Information accessed by unauthorized parties	Low
R12	Software failure	Low
R13	Data backup failure	Low
R02	Strong winds	Medium
R08	New information technology staff don't understand how the system works yet	Medium
R14	Unstable internet network	Medium
R15	Server down	Medium
R03	Lightning	High
R09	Admin negligence in the process of updating data and information	High
R11	Hardware damage	High
R16	Power outage	High

Referring to Table 9, it is evident that out of the 16 potential information technology risks present in an educational institution in Indonesia, 8 of them fall into the low-risk category. These risks encompass factors such as fire, earthquake, inadequate human resources in terms of both quality and quantity for information technology, unscheduled system maintenance processes, logical attacks (hacking and malware), unauthorized access to information, software failures, and data backup failures. Additionally, there are 4 risks categorized as medium-level risks, including strong winds, new information technology staff lacking understanding of system operations, unstable internet network, and server downtime. Furthermore, 4 risks are classified as high-level risks, namely lightning strikes, administrative negligence in updating data and information, hardware damage, and power outages.

3.2. Risk Treatment

The subsequent stage in the analysis of information technology risk management within an educational institution in Indonesia is risk treatment. This phase entails providing recommendations concerning the treatment of all potential information technology risks at the institution. The proposed treatments aim to minimize the likelihood of risks occurring and mitigate their potential impacts. By implementing these measures, it is expected that the application system will function optimally, and the organization's business processes will remain uninterrupted. Specific details of the proposed treatments can be found in Table 10.

Table 10. Proposed Risk Treatment

ID	Possible Risks	Risk Level	Risk Treatment
R01	Fire	Low	Prepare firefighting equipment in various locations, especially in school buildings. Provide a backup server in a safe place and different from the main server. Perform database mirroring techniques on the backup server against the school's main database so that the backup server also stores data contained on the main server.
R04	Earthquake	Low	Provide a backup server in a safe place and different from the main server. Perform database mirroring techniques on the backup server against the school's main database so that the backup server also stores data contained on the main server.
R05	Lack of human resources in the information technology section in quality and quantity	Low	Provide training and guidance to school staff and teachers on matters relating to the operation of information technology.
R06	Unscheduled system	Low	Make a definite and routine system maintenance schedule every day.

ID	Possible Risks	Risk Level	Risk Treatment
	maintenance process		Maintenance process when school activities are over.
R07	Logical attacks (hacking and malware)	Low	Provide passwords as unique and difficult as possible for every important part of the server computer owned by the school. Activate firewall and internet security on the school server computer. Scan all computers using a quality antivirus program on a regular basis.
R10	Information accessed by unauthorized parties	Low	Urge all users of the school's application system not to provide usernames and passwords to other people. Provide access restrictions for each application system user.
R12	Software failure	Low	Immediately make improvements if there are deficiencies or errors in the software.
R13	Data backup failure	Low	Ensure that the storage memory usage is not full. Increase storage memory capacity. Maintenance processes and data backups on a regular basis.
R02	Strong winds	Medium	Provide a backup server in a safe place and different from the main server. Perform database mirroring techniques on the backup server against the school's main database so that the backup server also stores data contained on the main server.
R08	New information technology staff don't understand	Medium	Provide training and guidance to new staff regarding SOP and how the system works on a regular basis

ID	Possible Risks	Risk Level	Risk Treatment
	how the system works yet		until new staff really understand this.
R14	Unstable internet network	Medium	Reduce network traffic. Internet Service Provider facilities that have better quality.
R15	Server down	Medium	Checking the school's main database regularly every day. Refreshing the use of logs, temp, and RAM from using the main application system and database to prevent server downtime. Scan the server computer using a quality antivirus program on a regular basis.
R03	Lightning	High	Install lightning protection tools and equipment. Provide a backup server in a safe place and different from the main server. Perform database mirroring techniques on the backup server against the school's main database so that the backup server also stores data contained on the main server.
R09	Admin negligence in the process of updating data and information	High	Make a schedule for the admin so that the admin updates data and information regularly every day. Check data and information regularly every day. Check and ensure that the data and information to be input is in accordance with reality and facts.
R11	Hardware damage	High	Hardware checks and maintenance on a regular basis. Use existing hardware in schools carefully.

ID	Possible Risks	Risk Level	Risk Treatment
			Maintain cleanliness around the hardware area.
R16	Power outage	High	Providing a generator set that has power according to the needs and conditions of the organization, as well as installing an UPS (Uninterruptible Power Supply).

The implementation of the recommended treatments allows the institution to proactively address the identified risks and enhance the overall resilience of its information technology infrastructure. The treatments effectively mitigate risks such as fire, earthquake, lack of human resources, unscheduled system maintenance, logical attacks, unauthorized access, software failures, and data backup failures, all of which are categorized as low-level risks. These risks are effectively addressed through a combination of measures, including enhancing physical security, implementing regular system maintenance, robust cybersecurity measures, and proper data backup procedures.

Furthermore, medium-level risks such as strong winds, lack of understanding among new information technology staff, unstable internet network, and server downtime require specific attention. To mitigate these risks, the proposed treatments focus on stabilizing the network infrastructure, providing comprehensive training programs for new staff members, and establishing redundant systems to minimize server downtime. Additionally, high-level risks including lightning strikes, administrative negligence, hardware damage, and power outages require critical actions to mitigate their potential impacts. The institution may consider implementing lightning protection systems, enforcing strict administrative procedures, ensuring regular hardware maintenance and inspection, and establishing backup power sources to effectively address these risks.

The risk treatment stage plays a vital role in aligning the institution's risk management efforts with the specific information technology risks identified. The proposed treatments aim to reduce the likelihood of risks occurring and minimize their potential impact, enabling the institution to maintain optimal functioning of its application systems and ensure uninterrupted business processes. It is crucial for the institution to carefully evaluate the proposed treatments, taking into account their feasibility, cost-effectiveness, and alignment with the overall risk management strategy. Regular reviews and updates to the risk treatment plan are essential to adapt to evolving information technology risks and ensure continued effectiveness in managing these risks. By diligently implementing the recommended treatments and continuously monitoring and reassessing information technology risks, the educational institution can strengthen its resilience, protect valuable assets, and safeguard the continuity of its operations in an increasingly technology-driven environment. This proactive approach to risk treatment contributes to the institution's overall risk management framework and fosters a culture of resilience and security within the organization.

4. CONCLUSION

The analysis of information technology risk management stages has been successfully conducted at an educational institution in Indonesia. The process involved the comprehensive assessment of risks, starting from the risk identification, analysis, and evaluation stages. Subsequently, the risk treatment stage provided valuable recommendations for addressing the identified information technology risks within the institution. The research findings reveal a total of 16 possible information technology risks that have the potential to disrupt the institution's business processes. Among these risks, 8 were classified as low-level risks, including fire, earthquake, insufficient human resources in the information technology department, unscheduled system maintenance, logical attacks, unauthorized access, software failures, and data backup failures. Additionally, 4 risks were identified at the medium level, including strong winds, lack of understanding among new information technology staff, unstable internet network, and server downtime. Furthermore, 4 risks were categorized as high-level risks, namely lightning strikes, administrative negligence in updating data and information, hardware damage, and power outages.

To mitigate these risks, the educational institution has implemented appropriate measures; however, it should be acknowledged that the mitigation process is primarily based on experience and carried out periodically. The results of this research aim to support educational institutions in identifying potential risks within their organizations and formulating effective policies to address these risks. By doing so, organizations can minimize the occurrence and impact of information technology risks in the future. It is recommended that educational institutions further enhance their risk management practices by adopting a proactive and continuous approach. By utilizing the findings and recommendations of this research, institutions can strengthen their resilience against information technology risks, ensuring the uninterrupted operation of their business processes. Additionally, the integration of standardized risk management frameworks, such as ISO 31000, can further enhance the effectiveness of risk mitigation efforts and provide a structured approach to managing risks in the future.

REFERENCES

[1] M. S. Haq, "Implementasi Sistem Informasi Manajemen Dalam Meningkatkan Pelayanan Pendidikan Sekolah Di Masa Pandemi Covid-19," Jurnal Inspirasi Manajemen Pendidikan, vol. 9, no. 5, pp. 1221-1235, 2022.

[2] T. Ramdhany and R. A. Krisdiawan, "Analisis Risiko Sistem Informasi Penjualan Berbasis Iso 31000 - Risk Management di PT. Remaja Rosdakarya," JEJARING : Jurnal Teknologi dan Manajemen Informatika, vol. 3, no. 1, p. 1–7, 2018.

[3] T. F. Rahardian and A. F. Wijaya, "Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000," Journal of Information Systems and Informatics, vol. 4, no. 2, pp. 428-443, 2022.

[4] S. W. D. Read, The Practice of Risk Management, Euromoney Book, 2004.

[5] D. Prabowo and A. F. Wijaya, "Risk Management Analysis on KKM LKF FTI UKSW Website Using ISO 31000 Framework," Journal of Information Systems and Informatics, vol. 4, no. 1, pp. 65-76, 2022.

[6] ISO, "ISO 31000:2018(en) Risk management — Guidelines," Online Browsing Platform (OBP), 2018.

[7] D. L. Ramadhan, R. Febriansah and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," JURIKOM (Jurnal Riset Komputer), vol. 7, no. 1, pp. 91-96, 2020.

[8] Z. A. Hasibuan, Metodologi Penelitian di Bidang Ilmu Komputer dan Teknologi Informasi, Konsep, Metode Teknik dan Aplikasi, Depok, 2007.

[9] Y. N. Qintharah, "Perancangan Penerapan Manajemen Risiko," JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi, vol. 10, no. 1, pp. 67-86, 2019.

[10] S. Agustinus, A. Nugroho and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 1, no. 3, pp. 250-258, 2017.

[11] P. Kanantyo and F. S. Papilaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," JATISI (Jurnal Teknik Informatika dan Sistem Informasi), vol. 8, no. 4, pp. 1896-1908, 2021.

[12] R. Maralis and A. Triyono, Manajemen Risiko, Yogyakarta: Deepublish, 2015.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

[13] F. N. Indroes, Manajemen Risiko Perbankan : Pemahaman Pendekatan 3 Pilar Kesepakatan Basel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesia, Delok: Rajawali Pers, 2011.

[14] W. N. Cahyo, Framework Peningkat Kinerja Sistem Manajemen Aset Berbasis ISO 55001 dan ISO 31000, Yogyakarta: Universitas Islam Indonesia, 2020.

[15] I. Bafadhol, "Lembaga Pendidikan Islam di Indonesia," Edukasi Islami: Jurnal Pendidikan Islam, vol. 6, no. 11, pp. 59-72, 2017.