DOI: https://doi.org/10.33197/justinfo.v2i1.1743 ISSN: 3031-3449

Risk Management of Outdoor Equipment Rental Information System Using NIST SP 800-30 Framework at PT. XYZ

[1]Muhammad Adib Septiawan, [2]Agustian Dermawan, [3]Aulia Nur Adib Phasya, [4]Agus Arif Adipermana, [5]Ucu Nugraha

[1] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, adib.septiawan@widyatama.ac.id
[2] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, dermawan.agustian@widyatama.ac.id
[3] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, nur.adib@widyatama.ac.id
[4] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, agus.arif@widyatama.ac.id
[5] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

The implementation of an information system in a company has benefits as well as threats that can have a negative impact if appropriate risk handling is not carried out. This research will conduct risk management of the information system of an outdoor activity service rental company using the NIST SP 800-30 framework. The goal is to identify risks that may arise in the company and provide appropriate actions for each of these risks. The results of risk management show the threats faced by the company, such as natural disasters, physical security and cyber security with most of these risks being high-level risks. The final result is in the form of providing recommendations that can be done by the company to minimize the resulting impact and the chances of these risks occurring. Thus, the company's business activities and activities can run well.

Keywords: Risk Management, NIST SP 800-30, Risk Assessment, Information System.

Corresponding Author:

Ucu Nugraha
Information Systems, Faculty of Engineering, Widyatama University
Bandung, Indonesia
ucu.nugraha@widyatama.ac.id

INTRODUCTION

PT. XYZ is a service business that not only offers camping equipment rental, they also try to develop mountain climbing guide services and outdoor clothing manufacturing in the city of Bandung. PT. XYZ has an information system that allows organizations to have neatly arranged daily activities and the management of data owned and stored by the organization.

Rapidly developing technology not only has a good impact, but also has a negative impact that never existed before. This can be a threat and a risk that has the potential to hinder activities and activities at PT. XYZ. Previously, PT. XYZ had never carried out activities related to the risk management process. Without risk management activities in an organization or company, they will not be able to track what threats can occur and the impacts they have on them. Therefore, this study will conduct a risk management analysis at PT. XYZ to find out what risks can threaten PT. XYZ, how big the probability and impact can be from known risks and can provide guidance to PT. XYZ regarding what actions should be taken to minimize the impact and opportunities for these risks to occur.

The framework that will be used in conducting risk management analysis at PT. XYZ is the NIST 800-30 framework. The NIST 800-30 framework is used because it has one advantage compared to other risk management frameworks, namely a comprehensive process and risk management analysis that can be adjusted to the circumstances of the organization[1].

LITERATURE REVIEW

An information system is a system created by humans and consists of various elements within an organization with the main aim of providing information. According to Anggraeni and Irviani (2017), an information system is a structured combination of individuals, hardware, software, communication networks, and data resources that systematically collect, process, and disseminate information within an organization. According to Ardana and Lukman (2016), an information system is a structure consisting of interconnected components, which are tasked with collecting (and retrieving), processing, storing, and distributing information to support the decision-making and control process in a company. According to Pradana and Waspada (2019), an information system is a data relationship supported by software and hardware to present information that supports decision making. It helps in carrying out activities by considering time aspects, both in the short, medium, and long term. In the context of an organization, all elements connected in this information system play a role in helping to carry out the organization's business activities. According to Shadek and Swastika (2017), an information system is the result of human construction in the form of elements within an organization, aimed at achieving a specific goal, namely presenting information. The parts of this information system involve hardware, software, data, and procedures.

According to the Big Indonesian Dictionary, rent is payment or wages for the use of something, an agreement or contract regarding the use of something with payment, and the act of obtaining rights or permission to use something by paying money or renting something to another party. According to Septavia et al. (2016), renting can be defined as an agreement or consent in which one party agrees to provide an object to another party, so that the second party can use the object for a certain period of time, with the obligation to pay an agreed rental fee. According to Pradana and Waspada (2019), renting can be explained as an agreement in which a certain party commits to providing an item for a certain period of time to another party, in exchange for payment of a rental price that has been agreed upon and approved by the party willing to pay it. According to Frayoga and Fitriani (2016), Renting is a process or method of renting or leasing. Rent is a service fee for the use of a room in an empty state that can be paid in advance (at the beginning of the rental) or in arrears according to the agreed contract or agreement. According to Septiani et al. (2019) , Leasing is a contract in which the lessor has the right to use an asset for a certain period of time. In return, the lessor makes a payment or series of payments to the lessor. According to Prasetyo and Nawawi (2022), Renting is an agreement in which the owner of a property or asset agrees to use it by another party for a certain period of time. The goods or services being rented vary, and there are various choices of duration and different rental rates.

Risk is related to uncertainty, it occurs because of the lack or unavailability of sufficient information about what will happen. Something that is uncertain can result in benefits or losses. Risk is a danger, consequence or consequence that can occur as a result of an ongoing process or future event, or can be interpreted as a state of uncertainty, where if an undesirable situation occurs it can cause loss. According to Ucu and Rozahi (2019) Risk is a danger, result, or consequence that can occur as a result of an ongoing process or future event, or can be interpreted as a state of uncertainty, where if an undesirable situation occurs it can cause losses. According to Sudarmanto et al. (2021), risk is an event that has not (possibly) occurred but has the potential to affect certain goals. The impact of the event can be positive or negative. According to Latifiana (2016), risk is the possibility of an adverse event occurring for a company or business, where the event cannot be predicted. According to Sidik and Wahyuari (2023), risk can generally be explained as uncertainty related to potential financial losses or the possibility of losses. This uncertainty can come from various factors, such as uncertainty in economic conditions, natural conditions, accidents, criminal acts such as murder or theft, and so on. According to Arifudin et al. (2020), risk can be interpreted as an event that results in losses or differences in results from those expected.

According to Fahmi (2010), risk management is a field of science that discusses how an organization or company applies measures to manage risks that may be faced. Risk is related to uncertainty, and risk management aims to manage these risks so that they do not have a detrimental impact. According to the Financial Services Authority (2016), risk is the possibility of an undesirable outcome that can cause a loss. Risk is related to uncertainty, and risk management aims to manage the risk so that it

does not have a detrimental impact. According to Rustam (2017), risk management is a series of methodologies and procedures for measuring, monitoring and controlling risks arising from all business activities, including credit risk, market risk, operational risk and other risks in an effort to maximize the company's value. Management Information System is one of the fields of study that is currently developing rapidly along with the development of information technology. This system requires development due to progress and development in terms of technology, social, culture, consumer demand, level of competition, and others. The risk management process includes the application of policies, procedures, and practices to carry out context setting, risk identification, risk analysis, risk evaluation, and risk treatment. Integration is the keyword and characteristic of risk management. All members of the organization must have an awareness and concern for risk and how risk and risk management should be placed in the perspective of the entire organization and Owner Unit.

METHODOLOGY

This study applies a qualitative method with a case study approach. The research was carried out carefully, in-depth, and comprehensively by conducting in-depth interviews and direct observations, and describing aspects related to the research subject. The main focus of the study is IT risk management at PT. XYZ, using the NIST SP 800-30 framework. The data collection stage is carried out by conducting direct observation of the rental system in PT. XYZ and conducting interviews with employees from PT. XYZ. At this stage, information is also collected regarding any problems that occur in the system, how the company controls it and how big the impact is for the company. NIST issued recommendations through a special publication 800-30 containing how to carry out risk management using the NIST 800-30 framework issued in 2002 with the title Risk Management Guide for Information Technology System. There are 9 processes in risk management. Here is a more detailed explanation of the nine steps in the NIST method:

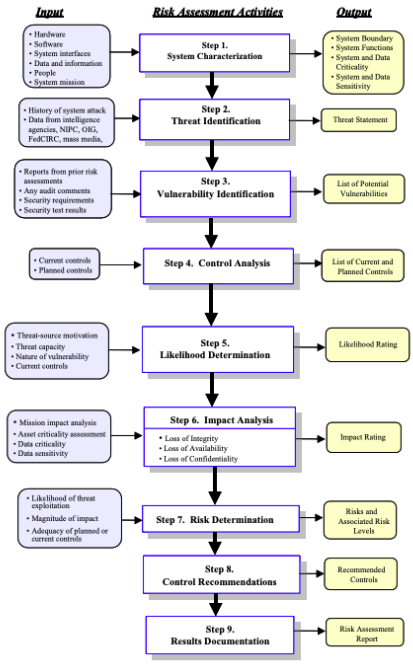

Figure 1. NIST SP 800-30 Risk Assessment

1. System Characterization: In assessing risk for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and information that make up the system. Describing an IT system establishes the scope of the risk assessment effort, describes the boundaries of operational authorization (or accreditation), and provides information (such as hardware, software, system connectivity, and responsible division or support personnel) that is essential to defining the risk.

2. Threat Identification: Threat identification is the potential of a particular threat source to successfully exploit a particular vulnerability. A vulnerability is a weakness that can be triggered accidentally or exploited intentionally. A threat source does not present a risk when there is no vulnerability that can be exploited. In determining likelihood , one must consider the threat source, potential vulnerabilities, and existing controls.
3. Vulnerability Identification: The analysis of threats to an IT system should include an analysis of the vulnerabilities associated with the system's environment. The purpose of this step is to develop a list of system vulnerabilities (weaknesses or weaknesses) that could be exploited by potential threat sources.
4. Control Analysis: The purpose of this step is to analyze the controls that have been implemented, or are planned to be implemented, by the organization to minimize or eliminate the possibility (or probability) of threats exploiting system vulnerabilities.
5. Likelihood Determination: To obtain an overall likelihood determination indicating the probability that a potential vulnerability could be exploited within the framework of the associated threat environment, the following governing factors should be considered: the motivation and capabilities of the threat source, the nature of the vulnerability, and the existence and effectiveness of current controls. The likelihood that a potential vulnerability could be exploited by a particular threat source can be described as high, medium, or low.
6. Impact Analysis: The next major step in measuring the level of risk is to determine the adverse impact that would result from a threat successfully exploiting a vulnerability. To do this, it is important to know how the system processes the vulnerability.
7. Risk Determination: The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of the probability that a particular threat source attempts to exploit a particular vulnerability. The magnitude of the impact if the threat source successfully exploits the vulnerability also needs to be considered. And finally the adequacy of planned or existing security controls to mitigate or eliminate the risk.
8. Control Recommendations: In this step, controls are created that can reduce or eliminate the identified risks, according to the organization's operations, provided. The purpose of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level.
9. Result Documentation: Once the risk assessment is complete (threat sources and vulnerabilities are identified, risks are assessed, and recommended controls are provided), the results should be documented in a formal report or information release. The risk assessment report is a management report that helps senior management, the mission owner, make decisions regarding policies, procedures, budgets, and operational changes and system management.

RESULTS AND DISCUSSION

The following is a discussion and results of the risk management analysis of the outdoor equipment rental information system at PT. XYZ.

1. System Characterization

This stage is carried out by identifying the assets owned to support the outdoor goods rental system in the company. The details of the assets are as follows: Data, Software (Microsoft Excel, web for blogs), hardware (a set of PCs), networks (UTP cables, RJ45, Routers), CCTV, Mobile phones, UPS.

2. Threat Identification

The next step is to identify what threats might attack the outdoor rental system starting from its type, examples of threats that occur and what are the consequences of the threat. Here are the details of the threat identification.

Table 1Threat Identification

Types of Threats	Examples of Threats	Consequences of Threats
Natural disasters	Earthquake, Landslide, Lightning, Fire.	Damage to facilities and disruption of business activities
Physical Security	Hardware Theft, Hardware Vandalism.	Loss of hardware or documents, hardware failure.
Cyber Security	Malware Attacks, Phishing.	Information theft, loss of critical data, unauthorized data changes, and system disruptions

It is known that the types of threats that can occur in the rental system can occur due to natural disasters such as earthquakes, landslides, lightning and fires. Physical security such as hardware theft and hardware destruction. And finally cyber security such as malware and phishing attacks.

3. Vulnerability Identification

In vulnerability identification, it is explained what risks can occur in the rental system and what impacts can occur if these risks occur in the system.

Table 2Vulnerability Identification

No	Risk	Impact
1	Landslide	Damage to infrastructure and utilities that disrupt business activities.
2	Lightning	Damage to computer devices.
3	Earthquake	Damage to infrastructure and utilities that disrupt business activities.
4	Fire	Damage to infrastructure and utilities that disrupt business activities.
5	Memory Full	New data input will experience delays in the presentation process.
6	Hardware Failure	Unable to access the system.
7	Data Corrupt	Inhibits the working system due to corrupted data.
8	Sudden Power Outage	All activities stopped.
9	Hardware Theft	Financial losses and business activities will be disrupted.
10	Lack of human resources in terms of quantity and quality	The data completion process is not timely, and there are errors in inputting, editing or deleting data.
11	Internet Disruption	Accessing the system takes a long time or stops and the rental system is hampered.

After conducting the threat identification process, it was discovered that there were eleven risks that could occur in the company's outdoor goods rental system.

4. Control Analysis

This stage is an analysis of the controls that the company has implemented in operating the company's outdoor goods rental system against the risks that occur.

Table 3Control Analysis

No	Risk	Control
1	Landslide	Conducting natural disaster simulation training for employees.
2	Lightning	Providing lightning protection equipment.
3	Earthquake	Conducting natural disaster simulation training for employees.
4	Fire	Keep electronic devices away from things that can trigger fires.
5	Memory Full	Always monitor memory usage. Clean memory if there is unnecessary data and enlarge memory capacity.
6	Hardware Failure	Repair damaged hardware. If it cannot be repaired, replace it immediately with a new one so as not to interfere with activities.
7	Data Corrupt	Perform regular data backups, perform scans using a licensed anti-virus

		regularly and clean your PC to prevent the emergence of viruses/malware that can cause data corruption.
8	Sudden Power Outage	Providing UPS for hardware.
9	Device Theft	Installing security systems such as CCTV and access restrictions (data, hardware).
10	Lack of human resources in terms of quantity and quality	Recruitment of new staff as needed. Conducting guidance (training) to new staff.
11	Internet Disruption	Use a quality internet service provider and optimize internal network settings to increase internet speed.

It can be seen that the eleven risks that occurred have been controlled by the company.

5. Likelihood Determination

The step in the risk management process where risks or possible events are evaluated based on how likely they are to occur. This is one of the elements used to measure the level of risk of a particular event or condition. Measured on a scale of low, moderate, or high.

Table 4. Likelihood Determination Parameters

Level of Probability	**Definition of Possibility**
Low	Low or low threat indicates that the possibility of a particular event or risk occurring is considered low or rare. With a frequency of less than 1 time per year.
Moderate	Moderate or medium threat indicates that the possibility of an event or risk occurring is at a moderate level, meaning it is not too high or low. With a frequency of 2 to 5 times a year.
High	High or high threat describes that an event or risk has a high possibility or is very likely to occur. With a frequency of more than 5 times a year

Then the scale of the risks is carried out based on the indicators in the table above. So that it can be seen that the risks are categorized as low, moderate or high.

Table 5. Likelihood Determination

No	**Risk**	**Probability of Threat Events Occurring**	**Possible Threats That Result in Negative Impacts**	**Overall Probability**
1	Landslide	Low	High	Moderate
2	Lightning	Low	High	Moderate
3	Earthquake	Low	High	Moderate
4	Fire	Low	High	Moderate
5	Memory Full	Moderate	Moderate	Moderate
6	Hardware Failure	Low	High	Moderate
7	Data Corrupt	Moderate	High	High
8	Power failure	Moderate	Low	Low
9	Hardware Theft	Low	High	Moderate
10	Lack of human resources in terms of quantity and quality	Low	Moderate	Low
11	Slow internet	High	Low	Moderate

It can be seen that the likelihood (tendency or opportunity) of the overall risk is likely to have two low scales, eight moderate scales and one high scale. This proves that the risk opportunities that occur have an average of moderate or medium.

6. Impact Analysis

At this stage, impact analysis is conducted to determine how big the impact will be if the existing risks occur. Measured on a scale of low, moderate, or high

Table 6Impact Analysis Parameters

Threat Level	Impact of Threats
Low	Threats or risks have a relatively small or limited impact on certain aspects of the organization.
Moderate	Threats or risks have a moderate impact and can affect several areas or functions within the organization.
High	Threats or risks have a significant or serious impact on the organization's operations, reputation, finances, or viability.

Then the scale of the risks is carried out based on the indicators in the table above. So that it can be known that the risks are categorized as low, moderate or high.

Table 7Impact Analysis

No	Types of Impact	Maximum impact	Information
1	Landslide	High	The impact is high because if an unexpected disaster occurs with an unexpected level of damage, there is a possibility of damage to existing assets and facilities.
2	Lightning	Moderate	The impact is moderate because lightning can disrupt networks, cause electrical disturbances, and can physically damage computer devices.
3	Earthquake	High	The impact is high because if an unexpected disaster occurs with an unexpected level of damage, there is a possibility of damage to existing assets and facilities.
4	Fire	High	The impact is high because if an unexpected disaster occurs with an unexpected level of damage, there is a possibility of damage to existing assets and facilities.
5	Memory Full	Moderate	The impact is moderate because if it happens it can cause a significant decrease in performance such as becoming unresponsive.
6	Hardware Failure	High	Because it may cause data loss or complete system failure, and recovery may take time.
7	Data Corrupt	High	Perform regular data backups, perform scans using a licensed anti-virus regularly and clean your PC to prevent the emergence of viruses/malware that can cause data corruption.
8	Power failure	Low	Save periodically to prevent data loss.
9	Device Theft Hard	High	Installing security systems such as CCTV and access restrictions (data, hardware) as well as data monitoring and performing regular data backups
10	Lack of human resources in terms of quantity and quality	Moderate	Recruitment of new staff as needed. Conducting research and guidance (training) to new staff.
11	Slow internet	Moderate	Use a quality internet service provider and optimize internal network settings to increase internet speed.

From the categorization results, it can be seen that the risk with a low scale is one, moderate is four and high is six. This proves that the impact of the risks that occur has an average of high.

7. Risk Determination

Risk determination is the stage of determining the overall risk of determining the probability and impact analysis that has been done. It can be seen from the table below, how to determine the overall risk of the risks that occur.

Table 8Risk Determination

		Impact		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

The following is a determination of the risks that occur in the outdoor equipment rental system at the company.

Table 9Risk Determination

No	Threat	Overall Possibilities	Levels Of Impact	Overall Risk
1	Landslide	Moderate	High	High
2	Lightning	Moderate	Moderate	Moderate
3	Earthquake	Moderate	High	High
4	Fire	Moderate	High	High
5	Memory Full	Moderate	Moderate	Moderate
6	Hardware Failure	Moderate	High	High
7	Data Corrupt	High	High	High
8	Sudden Power Outage	Low	Low	Low
9	Hardware Theft	High	High	High
10	Lack of Human Resources in Quantity and Quality	Low	Moderate	Low
11	Internet Disruption	Moderate	Moderate	Moderate

It can be seen that the overall risk is two low scales, three moderate scales and six high scales. This proves that the average risk that occurs in the rental information system is high, so better handling is needed to minimize these risks.

8. Control Recommendations

At this stage, it is a control recommendation that can be carried out by the company to minimize the risks in the outdoor equipment rental system in the company. The control recommendations given are only for moderate and high scale risks because for low scale risks, the control carried out is very good.

Table 10Control Recommendations

No	Threat	Risk Level	Recommendation
1	Landslide	High	Conducting natural disaster simulation training for employees regularly at least once every 4 months by inviting training teams from agencies related to natural disasters.
2	Lightning	Moderate	Using good quality lightning protection equipment
3	Earthquake	High	Conducting natural disaster simulation training for employees regularly at least once every 4 months by inviting training teams from agencies related to natural disasters.
4	Fire	High	1. Conducting natural disaster simulation training for employees regularly at least once every 4 months by inviting training teams from agencies related to natural disasters. 2. Providing light fire extinguishers (APAR) 3. Create regulations not to store flammable items around electronic goods/assets
5	Memory Full	Moderate	1. Add storage for data backup 2. Replace storage with a larger size
6	Hardware Failure	High	1. Hardware maintenance at least once a month 2. Replacing hardware with a high level of failure
7	Data Corrupt	High	1. Periodic checks for stored data 2. Perform regular data backups at least once every two weeks 3. Using a licensed antivirus
8	Hardware Theft	High	1. Installing security devices to prevent theft of goods (Example: CCTV, installing padlocks to reduce access from outside parties) 2. Create rules to limit who can access the hardware.
9	Internet Disruption	Moderate	1. Change provider that can provide faster internet 2. Installing wifi and router

9. Result Documentation

Evaluation is the final stage in risk management analysis using the NIST 800-30 framework. At this stage, an evaluation of previously recommended controls is carried out. For risks whose source of threat is from nature such as landslides, lightning, earthquakes, and fires, it can be done by training in natural disaster simulations, and buying or repairing damaged hardware . For risks related to data such as full memory and corrupt data can be handled by backing up and increasing storage capacity. Then for the risk of hardware damage can be overcome by checking or maintaining hardware and replacing hardware that has a high level of damage. And finally For threats related to physical crimes such as hardware theft can be done by installing security devices and creating rules restricting hardware access.

CONCLUSION

The results of the risk analysis show that PT. XYZ faces various threats, such as natural disasters, physical security, and cyber security. These risks are then categorized and evaluated for their impact and likelihood. The results show that most risks have a high level of impact and likelihood, requiring further attention and management. Control recommendations are provided for moderate and high risks. These controls involve employee training, use of countermeasures, hardware maintenance, routine data backup, and physical security measures. Overall, this provides an overview of PT. XYZ need to improve its understanding and implementation of risk management, especially in the face of complex threats. Control recommendations can be a guide to minimizing the impact of risks and ensuring PT. XYZ business continuity.

REFERENCES

[1] Anggraeni, EY, and Irviani, R. 2017. Introduction to Information Systems , Yogyakarta: Andi Publisher.

[2] Ardana, IC, and Lukman, H. 2016. Accounting Information Systems , Jakarta: Mitra Wacana Media.

[3] Arifudin, O., Wahrudin, U., and Rusmana, FD 2020. Risk Management , Bandung: Widina Bhakti Persada Publisher.

[4] Elanda, A., & Buana, RL (2021). Infrastructure Risk Management Analysis Using NIST (National Institute of Standards and Technology) SP 800-30 Method (Case Study: STMIK Rosma). Elkom: Electronics and Computer Journal, 14(1), 141–151. https://doi.org/10.51903/elkom.v14i1.387

[5] Frayoga, DM, and Fitriani, L. 2016. "Design and Construction of Desktop-Based Camping Equipment Rental and Data Management Applications at the Individual Company Rz Adventure," Jurnal Algoritma (13:1), pp. 198–204. (https://doi.org/10.33364/algoritma/v.13-1.198).

[6] Latifiana, D. 2016. "Study of Financial Literacy of Small and Medium Enterprises (SMEs) Managers," National Seminar on Economic and Business Education , pp. 1–7.

[7] Mahatmyo, A. 2014. Accounting Information Systems: An Introduction , Deepublish.

[8] Pradana, DI, and Waspada, I. 2019. "Hybrid Application in Book Rental Information System," Simetris: Journal of Mechanical, Electrical and Computer Science Engineering (10:1), pp. 1–14. (https://doi.org/10.24176/simet.v10i1.2600).

[9] Prasetyo, DR, and Nawawi, M. 2022. "Development of Futsal Field Rental Information System at Maninjau Futsal," Jurnal Tekno Insentif (16:2), pp. 129–138. (https://doi.org/10.36787/jti.v16i2.886).

[10] Septavia, I., Gunadhi, E., and Kurniawati, R. 2016. "Web-Based Car Rental Information System at Jasa Karunia Tour And Travel," Jurnal Algoritma (12:2), pp. 534–540. (https://doi.org/10.33364/algoritma/v.12-2.534).

[11] Heavy Equipment Rental Information System ," JUSIM (Musirawas Information System Journal) (04:02), pp. 127–134. (https://jurnal.univbinainsan.ac.id/index.php/jusim/article/view/639).

[12] Shadek, TF, and Swastika, R. 2017. "Development of E-Learning System Applications in All Courses Using Hypertext Preprocessor (Php) Program in Order to Improve the Quality of Learning Process and Results," ProTekInfo (Informatics Engineering Research and Observation Development) (4), pp. 12–18. (https://doi.org/10.30656/protekinfo.v4i0.407).

[13] Soputan, G., Sompie, B., and Mandagi, R. 2014. "Occupational Health and Safety (K3) Risk Management (Case Study on the Construction of Eben Haezar High School Building)," Jurnal Ilmiah Media Engineering (4:4), pp. 229–238.

[14] Sudarmanto, E., Astuti, Kato, I., Basmar, E., Simarmata, HMP, Yuniningsih, Irdawati, Wisnujati, NS, and Siagian, V. 2021. Banking Risk Management , Kita Menulis Foundation.

[15] Syahrial Sidik, SS, and Wahyuari, W. 2023. "Risk Management of Online Examination Information Systems at Trisakti Insurance Management College," Journal of Green Growth and Environmental Management (12:1), pp. 84–97. (https://doi.org/10.21009/10.21009/jgg.v12i1.06).

[16] Ucu, N., and Rozahi, I. 2019. " Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment," International Journal of Advanced Science and Technology (28:6), pp. 140-145.