

## ISO 31000:2018-Based IT Infrastructure Risk Management Study (Case Study: Universitas Mikroskil)

Elly<sup>1</sup>, Hanes<sup>2</sup>, Joosten<sup>3</sup>

Information System  
Universitas Mikroskil  
Kota Medan, Indonesia

<sup>1</sup>elly@mikroskil.ac.id, <sup>2</sup>hanes@mikroskil.ac.id, <sup>3</sup>joosten.ng@mikroskil.ac.id

(\*) Corresponding Author

### Abstract

In dealing with risks, organizational stakeholders will need risk management to ensure that risks within the organization have been identified and appropriate controls have been implemented in each implementation of the organization's IT infrastructure. Risk management is a process of identification, analysis, assessment, control, and efforts to avoid, minimize, and even eliminate unacceptable risks. Implementation of risk management with ISO 31000 by risk analysis and the areas that will be the focus of risk management. Mikroskil University requires risk management standards to minimize the risk of using the internet and servers in academic activities required by all academic levels at Mikroskil. The stages of the research method that are by the chosen method are collecting the risks faced by the organization, determining the risk scale, and using a risk matrix for risk management priority exposure. The results of the risk management analysis are in the form of the basic principles of implementing risk management with the ISO 31000 standard, which is a recommendation to the organization in managing risk by applicable standards. The result of the risk level is two possible risks with a low level, ten with a high level, and 3 with an extreme level.

Keywords: ISO 31000, Risk, Risk management

### Abstrak

Dalam menghadapi risiko, para *stakeholder* organisasi akan membutuhkan pengelolaan risiko untuk memberikan jaminan bahwa risiko dalam organisasi telah diidentifikasi dan pengendalian yang tepat telah diterapkan dalam setiap implementasi infrastruktur TI organisasi. Manajemen risiko adalah suatu proses identifikasi, analisis, penilaian, pengendalian, dan upaya menghindari, meminimalisir, bahkan menghapus risiko yang tidak dapat diterima. Penerapan manajemen risiko dengan ISO 31000 sesuai dengan analisis risiko serta bidang yang akan menjadi fokus pengelolaan risiko. Universitas Mikroskil dalam penanganan risiko terkait infrastruktur TI memerlukan standar manajemen risiko untuk dapat meminimalkan risiko penggunaan internet dan server dalam aktivitas akademis yang diperlukan semua jajaran akademis di Mikroskil. Tahap – tahap metode penelitian yang sesuai dengan metode yang dipilih adalah pengumpulan risiko yang dihadapi organisasi, menentukan skala risiko, dan menggunakan matriks risiko untuk pemaparan prioritas penanganan risiko. Hasil dari analisis manajemen risiko berupa prinsip dasar penerapan manajemen risiko dengan standar ISO 31000 yang adalah rekomendasi kepada pihak organisasi dalam pengelolaan risiko sesuai dengan standar yang berlaku. Hasil dari tingkat risiko adalah 2 kemungkinan risiko dengan level rendah, 10 kemungkinan risiko dengan level tinggi, dan 3 kemungkinan risiko dengan level ekstrim.

Kata kunci: ISO 31000, Manajemen risiko, Risiko

### INTRODUCTION

The use of information technology has risks for the organization. Risk also has an impact that causes threats to the organization that affects decision-making (Pardjo, 2017). Organizations must prepare countermeasures if a risk occurs in utilizing the organization's Information Technology (IT)

infrastructure. The first step in managing the risks within the organization is to measure the risk of information technology (Candra et al., 2019).

In the millennial era, combined with the industrial revolution 4.0, information technology and telecommunications development has penetrated worldwide. Industrial revolution 4.0 combines automation technology with cyber



technology, now known as the internet (Cantoni & Tardini, 2006; Kurniawan & Rofiah, 2020; Mudawamah, 2020). The internet is a global communication network that connects all devices, such as smartphones, laptops, personal computers (PCs), and others. Using the internet in human life is like a primary need, where the internet plays a vital role in human activities (Ramadhan et al., 2020).

Universitas Mikroskil, one of the universities in Medan, has a part in the organizational structure managing information systems and information technology, namely the Information Systems and Digital Transformation Section (SITD). In managing the academic information system at Universitas Mikroskil, the SITD section manages the IT infrastructure, which is the organization's long-term asset. The current IT infrastructure management is carried out according to a routine process. There are several obstacles with routine activities carried out; among others, there is no handling if there is a power outage in the early morning hours. The server is left off until operational activities occur again during working hours using a generator. Procurement of hardware on the server is complex because it is difficult to import server equipment from local vendor organizations, which causes the server equipment provision time to take a long time to handle.

Regarding internet network infrastructure, there is no internet backup, which means that if the connection is disconnected from the provider, the connection in the organization will also immediately drop. From the problems above, the researcher took one of the risk management methods suitable for the above handling. The method chosen is ISO 31000, which can be used for organizations to minimize the risks and improve the security of information technology assets at Universitas Mikroskil, namely, servers and networks currently used. It is crucial to connect risk management with the objectives and outcomes at each organizational stage. A different measure of organizational performance is required to link risk management practices and their impact on performance. So need to do a study and research regarding the management and identification risks that Universitas Mikroskil will face to help the division solves all the problems and make priorities for which projects will be executed first.

Risk activities included in the risk management process, namely communication with stakeholders, which here is the SITD section, determining context, risk assessment, risk treatment, and monitoring and review. In addition, in the risk assessment, there is also a process of risk identification, risk analysis, and risk evaluation to see various possible risks and risk management

priorities (Agustinus et al., 2017; Rahmawati & Wijaya, 2019).

## RESEARCH METHODS

The method that the researcher will use leads to a risk management process according to the ISO 31000:2018 standard. The data collection technique involves interviewing the SITD division from the head division to the staff. The purpose of using this standard is to facilitate continuous improvement of server and internet management, improve the quality of organizational work, be responsive to changes, and focus on managing IT asset security (Adi & Susanto, 2017).

### Types of research

This study uses a qualitative approach so that the data collected is in the form of statements containing issues, problems, or problems that are by the situation, conditions, and facts within the organization.

### Research Target / Subject

The data collection technique used is the interview method. The target of this method is directed at the team in the Information Systems and Digital Transformation Section, starting from the ranks of the division heads to the staff who manage IT infrastructure such as servers and the internet at Universitas Mikroskil.

### Procedure

The following is a diagram of the research method that researchers, namely will carry out:

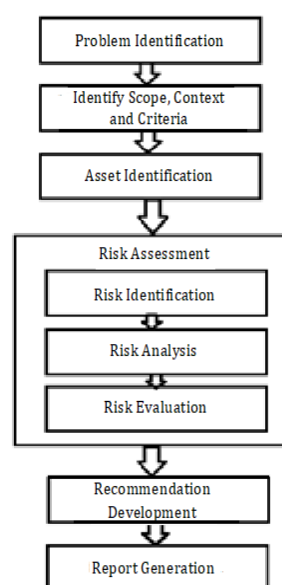


Figure 1. Research Flowchart

### 1. Problem Identification

In this stage, researchers collect and identify problems using interviews and literature studies with SITD starting from the Head of the Information System Center and its parts.

### 2. Identify Scope, Context, and Criteria

In this stage, the area to be analyzed is the SITD section. The external context analyzed by Universitas Mikroskil is network complexity and dependency on providers and hardware vendors. The internal context analyzed by Universitas Mikroskil is the vision, mission, and objectives of SITD, SITD organizational structure, risk management governance standards adopted by Universitas Mikroskil, and capabilities and knowledge related to server and internet utilization.

### 3. Asset Identification

Asset identification will cover three categories, namely:

- a. Technicals include hardware, processes, types of information, vendors, partners, and others.
- b. Physical includes the location of hardware and data and data center.
- c. People include asset owners and technical contacts.

### 4. Risk Assessment

#### a. Risk Identification

This stage identifies risks for assets that later relate to threats and impacts on the organization (Gilang M Husein & Radiant Victor Imbar, 2015). Will be formulated in the formula :

$$\text{Risk} = \text{Threat (condition)} + \text{Impact (consequence)}$$

#### b. Risk Analysis

This stage analyzes the risk assessment using a working paper containing a score or assessment with a Likert scale with low, moderate, and high scores (Angraini & Pertiwi, 2017).

#### c. Risk Evaluation

At this stage, all the analysis results will be compiled along with risk criteria for the presentation of decision options that can be chosen by the organization, such as no management action, considering risk recovery options, managing risk management controls for the future, and other things.

### 5. Recommendation Development

In this stage, the researcher will provide suggestions by the evaluation results and also communicate the activities and results of risk management to the organization, provide information for decision-making, and develop risk management activities in the form of risk

management standards that the organization can utilize.

### 6. Report Generation

In this stage, reports are developed for stakeholders, specific information on the needs and requirements, and the presentation of reports for related information for organizational purposes and decision-making.

## RESULTS AND DISCUSSION

Preparations that have been made and prepared to support this research include:

1. Asking permission from the SITD as the object of the research.
2. Conducting literacy studies on previous studies.
3. Determine the Research Context.

At this stage, the process of determining the goals of an organization will be carried out. A good management strategy is needed to achieve this goal so that the policies that will be taken can achieve organizational goals more optimally.

Strategic risk management includes all activities, such as identifying risks, solving problems, adapting to changes, and successfully implementing the plans that have been set (Okudan et al., 2021). The following are the components related to strategic risk management:

#### A. Strategic policy.

The strategic policy of SITD is stated in the SITD strategic plan (renstra) for 2016-2021. The policies are as follows:

1. Development of an integrated higher education management information system that can be accessed via a wide area network (WAN).
2. Utilization of information technology to support academic and organizational activities.
3. Utilization of environmentally friendly Information and Communication Technology (ICT).
4. Service recovery planning caused by the disaster.
5. Establishment of a mechanism to improve infrastructure security.
6. Increasing the capacity of IT services.
7. Improving the quality of SITD personnel.
8. Measuring the effectiveness of the application of ICT.

#### B. Resource

The resources available at SITD consist of:

1. Human Resources  
SITD personnel consists of 1 (one) Head of Center; 2 (two) Heads of Division; 6 (six)

Programmers; 4 (four) Information Technology Infrastructure Staff.

2. Facilities and infrastructure resources

SITD's facilities and infrastructure resources to date consist of: Common room for the Head of Center, Heads of Division, Programmers, and Information Technology Infrastructure staff with an area of 65.56 m<sup>2</sup>; Server room, with an area of 24.6 m<sup>2</sup>; Tables, Chairs, Cabinets, other office equipment/equipment for SITD personnel.

3. Information resources

To support their work, SITD personnel operate computers and equipment with the following details: Head of Center Computer 1 (one) unit, with 1 (one) unit network printer that is shared, connected to the internet. Head of Division 2 (two) computers connected to the internet. 6 (six) units of the Programmer's computers are connected to the internet. Information Technology Infrastructure Staff Computers 4 (four) units are connected to the internet. System development tools. Network administration tools and information technology services.

a. Organizational structure

The SITD unit consists of 1 Head of Section, which oversees 2 Heads of Subdivision, namely the Information System Development Subdivision and the Information Technology Infrastructure

Subdivision. Each field is assisted by staff called Programmers and Information Technology Infrastructure staff. SITD Organizational Structure can be seen in the following figure 2:

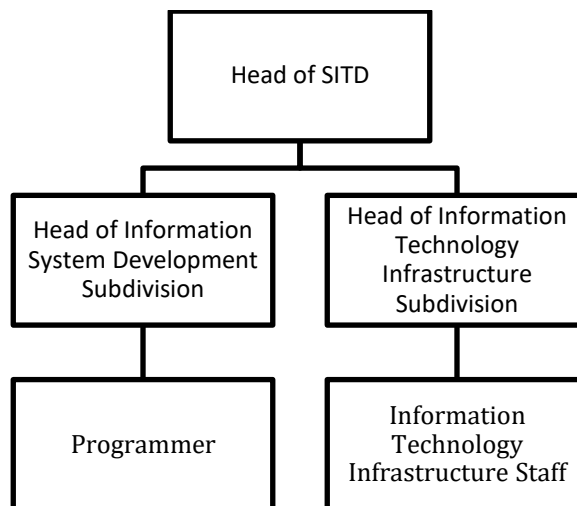


Figure 2. SITD Organizational Structure

The main task that is the responsibility of SITD is the management of information and communication technology. The tasks and functions performed can be seen in Table 1 below:

Table 1. Tasks and Functions SITD Organizational Structure

Position	Duties and responsibilities
Head of SITD	<ul style="list-style-type: none"> <li>Leading the implementation of the development and maintenance of information systems in support of the University's management, including implementing the Tri Dharma of Higher Education.</li> <li>Leading the evaluation of the implementation of the information system.</li> <li>Formulate and propose implementation guidelines for using information resources at the University.</li> <li>Establishing relationships/communication with other institutional information systems centers nationally and internationally.</li> <li>Prepare Work Plans and Budgets for information system development, operation, and maintenance activities.</li> <li>Receive and carry out other tasks ordered by the leadership.</li> <li>Report and be accountable for the implementation of their duties to the Head of SITD.</li> </ul>
Head of Information System Development Subdivision	<ul style="list-style-type: none"> <li>Manage the implementation of software development and information system databases required.</li> <li>Manage the implementation of software maintenance and information system databases.</li> <li>Create documentation about software and databases of information systems at the University.</li> </ul>

Continue Table 1. Tasks and Functions SITD Organizational Structure

Position	Duties and responsibilities
Head of Information System Development Subdivision	<ul style="list-style-type: none"> <li>• Support the implementation of data processing of the University's work units.</li> <li>• Receive and carry out other tasks ordered by the Head of SITD.</li> <li>• Report and account for the implementation of their duties to the Head of SITD.</li> </ul>
Head of Information Technology Infrastructure Subdivision	<ul style="list-style-type: none"> <li>• Manage information technology infrastructure services for the academic community.</li> <li>• Manage the implementation of planning and development of information networks.</li> <li>• Manage the implementation of development, maintenance, and documentation of the server room along with the hardware, system software, and computer networks in it.</li> <li>• Coordinate the implementation of communications to national and international scale information networks (such as: inherent), with the approval of the Head of SITD.</li> <li>• Receive and carry out other tasks ordered by the Head of SITD.</li> <li>• Report and account for the implementation of their duties to the Head of SITD</li> </ul>

b. Human Resources Capability

Workers in the SITD unit are workers who have experience in their fields. Heads of Sections and Heads of Subdivisions at SITD are S-2 and S-1 graduates from Universitas Mikroskil, which are part of Mikroskil's own family. Staff from each field are also Mikroskil students who have had achievements in several programming competitions. In addition, the staff is provided with skills from their respective fields.

c. System

Have communication lines between entities, operating systems, and delivery networks that are structured to support operational efficiency.

d. Identifying Risk

The company has an effective way of identifying the impact of economic conditions, competition, technology, laws, regulations, and other changes that can impact the achievement of organizational goals

IT infrastructure management is carried out according to routine processes. Some of the obstacles related to routine activities include: if there is a power outage in the early hours of the morning, there has been no handling. The server is left off until operational activities occur again during working hours using a generator. Procurement of hardware on the server is complex because it is difficult to import server equipment from local vendor organizations, which causes the server equipment provision time to take a long time to handle. Regarding internet network infrastructure, there is no internet backup, which means that if the

connection is disconnected from the provider, the connection in the organization will also immediately drop. The constraints mentioned above indicate that there are risks that impact Mikroskil's IT operational activities.

Therefore, an evaluation of server and network problems at Universitas Mikroskil was carried out according to the conditions faced by Mikroskil, especially during the current pandemic, which requires fast and precise risk management.

In this study, the research framework used by the researcher refers to ISO 31000, which is a guide to the application of risk, which consists of three elements, namely: framework, principles, and processes (Mahardika et al., 2019). ISO 31000 provides a risk management framework, principles, and processes that can be used as a risk management architecture and ensure the effective implementation of risk management in organizations. Risk management is identifying, measuring risks, and forming strategies to manage them through available resources. Risk management is needed to manage these risks to obtain optimal results. The risk management process includes five activities: communication and consultation, determining context, risk assessment, risk treatment, and monitoring and review, which is modified according to institutional needs.

The ISO 31000 chart (Pribadi & Ernastuti, 2020) (Pangestu et al., 2021), which was also modified according to the needs of this research, can be seen in Figure 3 below:



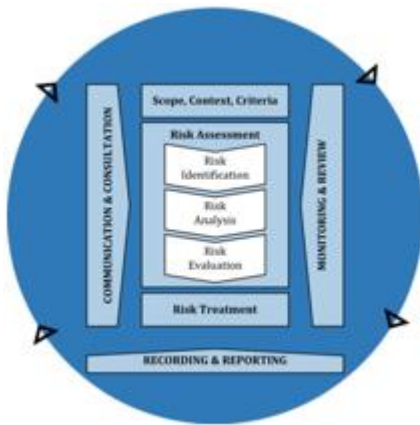


Figure 3. ISO 31000 Chart

Risk management involves systematically applying policies, procedures, and practices in communication and consulting activities, setting context, and assessing, reviewing, and reporting risks. The research framework can be seen in Figure 4 below:

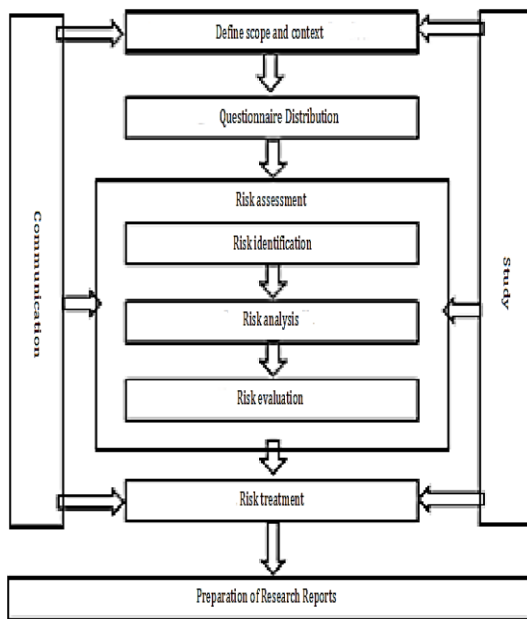


Figure 4. Research Framework

1. Communication

This stage is carried out at the research site for the Head of SITD. The data collection process was done through interviews, observations, and questionnaires to determine how to implement and handle risk management at Universitas Mikroskil.

2. Define scope and context

The determination of the scope is adjusted to problems related to risk on server and network

devices at Mikroskil. The determination of context is still focused on the internal environment of the institution in order to help achieve the objectives of the external context of Universitas Mikroskil.

3. Risk assessment

The risk assessment consists of three stages, namely:

a. Risk identification

The identification stage is carried out by finding out the IT assets in Mikroskil and knowing what risks are in the research area.

b. Risk analysis

After finding out the risks at Universitas Mikroskil, the next step is to analyze the impact on Mikroskil. The analysis activity is continued by taking into account the frequency of occurrence of risks and the value of the impact by using qualitative measures of probability and level of risk assessment.

c. Risk evaluation

This stage compares risks calculated based on risk and impact criteria by entering a qualitative risk analysis matrix.

4. Risk treatment

This stage is selecting options to minimize or eliminate the impact and possible occurrence of the risk.

5. Study

At this stage, studies are conducted periodically to obtain appropriate information on the needs and problems.

6. Preparation of Research Reports

After all, processes are completed, the researcher develops research reports by archiving and managing all research activities so that they can become valuable documents for Mikroskil.

The following steps that will be carried out in this research refer to the stages of ISO 31000, which have been described above, namely:

1. Risk Assessment

This stage is carried out to assess the risks that may occur to the existing IT infrastructure at Universitas Mikroskil. This stage is divided into three processes, namely:

a. Risk Identification

This process is carried out to identify risks that directly or indirectly impact business processes at Universitas Mikroskil. From the risks that have been identified, researchers will find out what actions have been taken to handle or minimize the impact of these risks.

b. Risk Analysis

Risk analysis is carried out to find out the risks that require special and appropriate handling so that the resulting impacts can be handled correctly or at least can be minimized. In this process, the

frequency of occurrence of risk will be calculated, and the magnitude of the impact of the risk will be measured. These two indicators will produce a list of possible risk assessments.

c. Risk Evaluation

The last process in the Risk Assessment stage is Risk Evaluation. This process uses a risk evaluation matrix divided into three levels: Low, Medium, and High. This matrix combines and adjusts the frequency value and the risk impact value with the values contained in the matrix. The result of this process is the risk level of each possible risk.

2. Risk Treatment

At this stage, the researcher will provide suggestions for actions that can be taken to assist in handling or minimizing the risks that may occur. In addition, the resulting suggestions can also be used to prevent these risks from occurring.

The results of the research carried out on the SITD started with an overview of the risks that arise for assets related to the Mikroskil information technology infrastructure system. Before identifying risks, it is necessary first to describe the IT assets related to servers and networks at Mikroskil. Table 3 shows a breakdown of the network devices used for the ICT infrastructure in Mikroskil.

Table 2. Network Devices

Device	Unit
Fiber Optic 1 Gbps	One lane
UTP Cat6e 1 Gbps	2 lane
Switch w/ FO converter	2 unit
Antenna Tower (40 m)	1 unit
Microtic Antenna 5,8 GHz	2 unit
Wireless Access Point	25 unit
Switch/Router	43 unit
Server Rack	1 unit
UPS (APC 5000VA)	1 unit
Video conferencing device (Polycom VSX 7400s)	1 unit
KVM Switch	1 unit
Storage - NAS	2 unit
Class Attendance Machine	48 unit
CCTV	4 unit
Employee Attendance Machine	2 unit
e-library tools	3 unit

Table 3 shows the list of server computers used to support information systems and information technology services for learning activities and other information technology services, including:

Table 3. Server Computers

Server	Jumlah
Server SIPT	1
Server Digital Library	1
Server SAP	1
Server Internet	3
Web Server	1
Mail Server	1
Database Server Web	1
WiFi Server (Captive Portal)	1
WiFi VPN	1
Radius Server	1
WiFi DNS Server	1
WiFi DHCP Server	1
Lab DNS Server	1
Key Management Service (KMS)	1
Network Time Protocol (NTP) Server	1
Cloud	1
MISO Server	1
Git Repository Server	1
IdeaFuse Server	1
DomJudge Server	1
DomJudge Host	15
Monitoring Server	1
Production Server	2

After identifying assets, what needs to be identified are the risks surrounding IT assets. Table 4 below is the result of observing risk identification using a questionnaire to the head of the SITD section.

Table 4. Result Risk Identification

Risk Identification List	
Source of Risk	Risk
<b>Nature/environment</b>	Lightning
	Variable Temperature
<b>People</b>	Human Error
	Data or information does not match the facts
<b>System and Infrastructure</b>	Server down
	Hardware failure or damage
	Overheat
	Network connection lost
	Overload
	Poor network quality
	Risk of damage due to mains voltage problems
	Poor system planning
	No priority system
	Lack of Human Resources
High dependence on SITD units	

Furthermore, in the risk analysis process, exposure to the impact of the identified risks is carried out. By studying the impact faced by



Mikroskil, it can be used as input and strategy for the decision-making process regarding risk. The findings on risk identification presented by SITD have an impact on risk management in Mikroskil.

The following Table 5 is a table of results from the identification of risk impacts:

Table 5. Identification Risk Impacts

Risk	Impact
<b>Lightning</b>	Lightning often causes the Public Router to be damaged so that system access from outside cannot be done.
<b>Variable temperature</b>	Temperatures that are too low cause the server to overheat and go down.
<b>human error</b>	Human error causes the system and infrastructure not to run as expected
<b>Data or information does not match the facts</b>	Data that does not match the facts can cause chaos at the stakeholder level.
<b>Server down</b>	Server down causes all information systems, and infrastructure can not to be used.
<b>Hardware failure or damage</b>	All information systems and infrastructure cannot be used at all.
<b>Overheat</b>	All information systems and infrastructure cannot be used at all.
<b>Network connection lost</b>	All information systems and infrastructure cannot be used at all.
<b>Overload</b>	Overload from the system side impacts all information systems, and infrastructure cannot be used at all, causing the server to go down.
<b>Poor network quality</b>	The lack of internet quality causes delays in distributing information to users and causes information system services not to work correctly.
<b>Damage due to power supply problems</b>	Unstable mains voltage can cause hardware damage.
<b>Poor system planning</b>	Poor planning causes a system that has been developed to be maintained repeatedly, hindering the completion of other work.
<b>No priority system</b>	The absence of a priority system causes units requesting services to be impatient and continue to pursue SITD units to complete their requests.
<b>Lack of human resources</b>	The shortage of human resources resulted in the completion of work cannot be carried out due to the high demand and the number of projects that were not proportional to the number of human resources
<b>High reliance on SITD units</b>	Since the average academic and non-academic activities at Universitas Mikroskil are already using information technology, the dependence of other units on the SITD unit is even greater. If there is a problem with the IT system or infrastructure, other units must wait for SITD to troubleshoot.

In the risk analysis stage, in addition to analyzing the impact, the researcher also assesses the frequency of risk occurrence and measures the risk impact assessment. The frequency of occurrence of risk is assumed to be within a period of 1 ( ) year.

The risk impact assessment measure uses the values below:

a. Score 1 (Insignificant): The risk does not interfere with business process activities

b. Score 2 (Minor): The risk of slightly hampering business processes

c. Score 3 (Moderate): Risk of disrupting business processes

d. Score 4 (Major): The risk of hindering certain parts of the business process

e. Score 5 (Catastrophic): The risk of hampering and disrupting all business processes



Measure the frequency of occurrence of risk using the values below:

- a. Score 1 (Rare): Can occur only in exceptional circumstances
- b. Score 2 (Unlikely): Likely to happen rarely
- c. Score 3 (Possible): It can happen once in a while
- d. Score 4 (Likely): Likely to happen often
- e. Score 5 (Almost Certain): Can happen any time

This assessment helps see the possibility of risk occurrence. Frequency and impact are filled with values from 1 to 5 according to the conditions described above. The greater the frequency value, the more often it occurs. Likewise, with the risk impact assessment where the greater the impact value means the risk is increasingly hampering and disrupting all business processes in Mikroskil. The following Table 6 is a table of the results of the assessment:

Table 6. Assessment's Results

Risk	Impact	Frequency
Lightning	5	3
Variable temperature	4	1
human error	4	4
Data or information does not match the facts	1	1
Server down	3	3
Hardware failure or damage	5	2
Overheat	4	2
Network connection lost	4	3
Overload	3	4
Poor network quality	2	2
Damage due to power supply problems	3	3
Poor system planning	2	4
No priority system	2	4
Lack of human resources	3	4
High reliance on SITD units	2	4

From the table above, we get the numbers showing the impact and occurrence frequency. The table above can be evaluated to determine how much risk is generated. This stage is called risk evaluation. The purpose of risk evaluation is to assist the decision-making process. Risk evaluation includes the process of comparing the results of the risk analysis of each risk against the risk criteria that have been established and then determining whether further action is required or not. Table 7 below describes the level of risk obtained. The risk levels in question are low, medium, high, and extreme.

Table 7. The Level of Risk

Risk	Impact	Frequency	Risk Level
Lightning	Catastrophic	Possible	Extreme
Variable temperature	Major	Rare	High
Human error	Minor	Likely	High
Data or information does not match the facts	Insignificant	Rare	Low
Server down	Moderate	Possible	High
Hardware failure or damage	Catastrophic	Unlikely	Extreme
Overheat	Major	Unlikely	High
Network connection lost	Major	Possible	Extreme
Overload	Moderate	Likely	High
Poor network quality	Minor	Unlikely	Low
Damage due to power supply problems	Moderate	Possible	High
Poor system planning	Minor	Likely	High
No priority system	Minor	Likely	High
Lack of human resources	Moderate	Likely	High
High reliance on SITD units	Minor	Likely	High

From the table above, it can be seen that there are:

- a. Two possible risks with a low level which means low-risk management can be carried out with routine procedures
- b. Ten possible risks with a high level which means high-risk management requires top management attention
- c. Three possible risks with extreme levels, which means extreme risk management needs to be done immediately

Regarding the results of risk evaluation, risk treatment can be carried out as an effort to select options that can reduce or eliminate the impact and possibility of the risk occurring. In general, there are four treatments, namely:

- a. Avoiding the risk means not carrying out or continuing the activities that give rise to the risk.
- b. Sharing risk means reducing the possibility of risk arising or the impact of risk on other parties
- c. Mitigation of risk means reducing the possibility of a risk arising or reducing the impact of a risk if it occurs, or reducing both
- d. Accepting the risk, means not doing any treatment for the risk

Risk management is focused on risks that are at the Extreme Level, then High, Medium, and then last are Low.

Table 8. Proposed Risk Treatment

Risk	Risk Level	Proposed Risk Treatment
<b>Lightning</b>	<i>Extreme</i>	<ul style="list-style-type: none"> <li>Setting up a backup server in a different location from the central server.</li> <li>Perform database mirroring techniques on the central database so that data stored on the primary server is also automatically stored on the backup server</li> </ul>
<b>Variable temperature</b>	<i>Extreme</i>	<ul style="list-style-type: none"> <li>Setting up a lightning rod</li> <li>Added parallel processing of temperature sensors to get accurate temperature data results</li> <li>Added temperature sensor and environmental data reader features</li> </ul>
<b>Human error</b>	<i>Extreme</i>	<ul style="list-style-type: none"> <li>Detect staff errors early by finding the root cause of problems in the work program.</li> <li>Provide proper training.</li> <li>Explaining the job desk of each human resource in the institution</li> </ul>
<b>Data or information does not match the facts</b>	<i>High</i>	Conduct regular checks on data and information related to information systems and technology
<b>Server down</b>	<i>High</i>	<ul style="list-style-type: none"> <li>Checking in 1 day period on the DB log, temp DB log, CPU usage, and RAM usage of the program and central database</li> <li>Refresh the DB log, temp DB log, CPU usage, and RAM usage of the main program and database.</li> <li>Install a quality antivirus so that it is not infected with malicious code</li> </ul>
<b>Hardware failure or damage</b>	<i>High</i>	<ul style="list-style-type: none"> <li>Maintain cleanliness and use of existing hardware.</li> <li>Immediately report to SITD staff if there is a hardware problem so that it can be addressed immediately</li> </ul>
<b>Overheat</b>	<i>High</i>	Prepare an air conditioning machine that suits your needs so that the hardware does not overheat
<b>Network connection lost</b>	<i>High</i>	Immediately report to the network handling section if it is felt that the connection is experiencing problems
<b>Overload</b>	<i>High</i>	<ul style="list-style-type: none"> <li>Arrange a schedule of checking in 1 day period on the DB log, temp DB log, CPU usage, RAM usage programs, and the central database</li> <li>Refresh the DB log, temp DB log, CPU usage, and RAM usage of the main program and database.</li> <li>Adding personnel in the database analyst section to be more alert in overcoming risks</li> </ul>
<b>Poor network quality</b>	<i>High</i>	<ul style="list-style-type: none"> <li>Improve network quality by collaborating with network providers.</li> <li>Perform regular network maintenance.</li> <li>Carry out complete and thorough testing and documentation of the network before it is put into operation</li> </ul>
<b>Damage due to power supply problems</b>	<i>High</i>	<ul style="list-style-type: none"> <li>Using stabilizers.</li> <li>Using UPS on technology devices</li> </ul>
<b>Poor system planning</b>	<i>High</i>	<ul style="list-style-type: none"> <li>The need for support from the leadership so that every department in the institution knows well the work procedures and the business processes' conditions.</li> </ul>



Continue Table 8. Proposed Risk Treatment

<b>Poor system planning</b>	<i>High</i>	<ul style="list-style-type: none"><li>• The database can be integrated and utilized correctly by all related parties</li><li>• The need for communication and transparency regarding the needs and needs of each department to cooperate with the SITD</li></ul>
<b>No priority system</b>	<i>High</i>	<ul style="list-style-type: none"><li>• Develop priority handling applications for problems related to systems and infrastructure being utilized.</li><li>• There is a notification feature for urgent complaints to the online complaint system at the institution</li></ul>
<b>Lack of human resources</b>	<i>Low</i>	<ul style="list-style-type: none"><li>• Recruiting new staff by setting standards that align with the institution's needs.</li><li>• Conducting staff training.</li><li>• Guide staff</li></ul>
<b>High reliance on SITD units</b>	<i>Low</i>	<ul style="list-style-type: none"><li>• Conducting training and guidance for staff, lecturers, and sections that require initial handling of the general equipment used in Mikroskil.</li><li>• Development of a support system to handle simple problems with IT services at Mikroskil</li></ul>

## CONCLUSIONS AND SUGGESTIONS

The implementation of risk analysis based on ISO 31000 gets three risk variables: nature and environment, human, system, and infrastructure. From the risk level assessment activities, it is also found that the level of risk that needs to be handled directly on three types of risk, among others: lightning, hardware failure or damage, and network connection is lost. Then ten types of risks require management attention: room temperature, human error, server down, overheating, overload, poor system planning, not having a priority system, lack of human resources, and dependence on the site team as well as two types of risks that only need to be handled regularly, such as data or information that does not match the facts and poor network quality. In the research, there are also weaknesses, where risk priorities are not calculated from studies of external parties who use the network so the results of risk priorities still require increased assessment in the future. The suggestions that can be given for future research are that the results of risk management analysis can be used as initiation documents or reference documents by Universitas Mikroskil in developing standard operating procedures (SOPs), risk management strategies, and business continuity planning (BCP) so that organizations can implement them.

## REFERENCES

Adi, D. E., & Susanto, N. (2017). Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar. *Jurnal Metris*, 18(1), 113–118.

- <http://mx2.atmajaya.ac.id/index.php/metris/article/download/2360/1105>
- Agustinus, S., Nugroho, A., & Cahyono, A. D. (2017). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*. <https://doi.org/10.29207/resti.v1i3.94>
- Angraini, & Pertiwi, I. D. (2017). Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan Iso 31000. *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi*, Vol. 3,(2). <https://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/4317>
- Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (2019). Sistem Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018. *Jurnal CoreIT*, 5(1). <https://garuda.kemdikbud.go.id/documents/detail/1219812>
- Cantoni, L., & Tardini, S. (2006). Internet. In *Internet*. <https://doi.org/10.4324/9780203698884>
- Gilang M Husein, & Radiant Victor Imbar. (2015). Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL). *Jurnal Teknik Informatika Dan Sistem Informasi*, 1. <https://journal.marannatha.edu/index.php/jutisi/article/download/575/571>
- Kurniawan, M. R., & Rofiah, N. H. (2020). Pola Penggunaan Internet di Lingkungan Sekolah Dasar Se-Kota Yogyakarta. *Southeast Asian Journal of Islamic Education*, 2(2), 93–105.



- <https://doi.org/10.21093/sajie.v2i2.1930>  
Mahardika, K. B., Wijaya, A. F., & Cahyono, A. D. (2019). Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000: 2018 (Studi Kasus: Cv. Xy). *Sebatik*, 23(1), 277-284. <https://doi.org/10.46984/sebatik.v23i1.572>
- Mudawamah, N. S. (2020). Perilaku Pengguna Internet : Studi Kasus Pada Mahasiswa Jurusan Perpustakaan Dan Ilmu. *BIBLIOTIKA : Jurnal Kajian Perpustakaan Dan Informasi*, 4(1), 107-113. <http://journal2.um.ac.id/index.php/bibliotika/article/download/14762/6000>
- Okudan, O., Budayan, C., & Dikmen, I. (2021). A knowledge-based risk management tool for construction projects using case-based reasoning. *Expert Systems with Applications*, 173. <https://doi.org/10.1016/j.eswa.2021.114776>
- Pangestu, R. H., Cahyono, A. D., & Tanaem, P. F. (2021). Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Menggunakan ISO 31000. *Journal of Computer and Information Systems Ampera*, 2(1). <https://doi.org/10.51519/journalcisa.v2i1.59>
- Pardjo. (2017). Manajemen Risiko Perusahaan. In *Tongue thrust and the stability of overjet correction*. [https://books.google.co.id/books?hl=id&lr=&id=AA1fDwAAQBAJ&oi=fnd&pg=PA89&dq=Manajemen+Risiko+Perusahaan&ots=0YovTUc4y6&sig=4WbnuFzywrWOSsbZ7LmpUpq-TYg&redir\\_esc=y#v=onepage&q=ManajemenRisikoPerusahaan&f=false](https://books.google.co.id/books?hl=id&lr=&id=AA1fDwAAQBAJ&oi=fnd&pg=PA89&dq=Manajemen+Risiko+Perusahaan&ots=0YovTUc4y6&sig=4WbnuFzywrWOSsbZ7LmpUpq-TYg&redir_esc=y#v=onepage&q=ManajemenRisikoPerusahaan&f=false)
- Pribadi, H. I., & Ernastuti, E. (2020). Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina). *Jurnal Sistem Informasi Bisnis*, 10(1), 28-35. <https://doi.org/10.21456/vol10iss1pp28-35>
- Rahmawati, A., & Wijaya, A. F. (2019). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP. *Jurnal SITECH: Sistem Informasi Dan Teknologi*, 2(1), 13-20. <https://doi.org/10.24176/sitech.v2i1.3122>
- Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer)*, 7(1), 91. <https://doi.org/10.30865/jurikom.v7i1.1791>