Service Risk Assessment Learning Management System using ISO 31000:2018/31010

Sri Hardianti
Departement of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Departement of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Many universities take advantage of the development of information technology to encourage the process of teaching and learning activities. Many models are used and one of them is LMS (Learning Management System). LMS (Learning Management System) is an electronic learning system program that is used to assist the learning process of students studying anywhere and anytime so that students can access material easily. One of them is LMS Ahmad Dahlan University which manages and implements website-based information technology using Moodle. Management cannot be separated from the possibility of risks that can disrupt the system and hinder learning business processes. Risk fixes should be scheduled so that when a breakdown occurs, recommendations can be made from the start and not when a risk occurs. Risk assessment using the 31000:2018 method is used for risk management guidelines which consist of communication and consultation stages, context setting, ISO 31010:2009 which is the standard assessment technique used consists of risk assessment stages (Risk identification, risk analysis, and risk evaluation), then the stages after the assessment are risk treatment, risk monitoring and review, risk recording and reporting using ISO 31000:2018 guidelines. Data was collected by filling out an introductory questionnaire and a questionnaire to identify the likelihood and impact of risks and determine stakeholders, RACI, and risk treatment and then validated through interviews with key informants. The results of this study are risk identification documentation that has 29 possible risk variables and risk impacts, and the results of the risk assessment of all variables are at a low level (low) but the risk management criteria are different, namely, 13 risks get a score scale of 1, and 16 risk gets a scale value 2 but at the same level. After being evaluated, the risk assessment can be used as a reference for preventing the handling and maintenance of information technology systems and assets in the future.

Keywords

LMS, ISO 31000, Risk Management, Risk Analysis

1. INTRODUCTION

Management System) which is an electronic learning system that is used to help students learn anywhere and anytime using the LMS system. Process management institutions are required to manage the importance of proper risk management. Maintenance of information technology assets is based on the problems that occur so it is urgent to carry out this assessment. A related problem obtained during the observation is that when there is an upgrade, the stakeholder section does not undergo an intense and in-depth discussion about the change, causing the system to fail. If this happens again in the future, an update failure may occur because no initial communication was made so that the resources department can make a backup first. The risk is initially low, eventually becomes high because the risk arises when recommendations are not given. Risk fixes should be scheduled so that when a breakdown occurs, recommendations can be made from the start and not when a risk occurs. For this reason, cooperation between the two fields is indispensable for ideal risk management, of course, by creating a good and structured flow of communication and consultation.

2. STUDY LITERATURE

2.1 Definition of Risk

Many various sectors have to face situations of increasing uncertainty, both in number, variety, and speed they turn into risks, problems, even crises and disasters for organizations [1]. Some of the drivers of the emergence of new sources of uncertainty are the development of digital technology, business process innovation, and the development of the millennial market which has very different expectations and guiding criteria from the previous generation [2].

2.2 Risk Assessment

Risk assessment can be concluded that a formal risk assessment will provide documentation to prove So that it can be interpreted, and the results will identify what treatment or what action should be taken which has been determined by management where the best decision is to accept those risks [3].

2.3 Risk Management

Risk management is an iterative process related to analysis, planning, implementation, control, and monitoring of policies and measurement of security implementation. This research will conduct a risk assessment using ISO 31000:2018/31010 which aims to document the risks. Every asset owned to all activities or processes that run in the company must have risks that can arise at any time without being predictable in advance that may arise [4].

2.3 Technology

Technology has become a means of generating needs from simple tools to large-scale human survival, the benefits of technology carry various sectors. Understanding technology is a collection of tools, rules, and procedures which are the application of scientific knowledge to a particular job under conditions that allow repetition [5].

2.3 Information

A collection of data or facts that have been processed into information for someone who accepts it [6]. Information is data that has been processed for use by someone to increase knowledge.

2.3Information Technology

Information technology is closely related to the development of computer technology and is integrated with telecommunications technology. With this formulation, the term information technology means the collection of data or facts that are processed and then converted or stored in the form of computer-based illustrated, video, text-based information. [7].

2.4 ISO 31000

The principles and guidelines in ISO 31000:2018 aim to provide principles and guidelines that are *generic* so that they can be used by all types of organizations without exception to deal with various risks that may arise in their [8]. The first risks based on SNI ISO 31000 are the risk management principles, the second is the risk management framework, and the third is the risk management process. Risk management based on SNI ISO 31000. Implementation of risk management using ISO 31000 is expected to be a guideline for risk management and how to prevent it. In general, ISO 31000 can be used and can also be specific in determining the appropriate technique for the agency. ISO 31000:2018 will be a general guide and ISO 31010:2009 will be a technique for conducting assessments [9].

2.5 Principles of Risk Management

There are always principles in each particular standard, the ISO 31000:2018 International Standard has implemented several principles that need to be met for risk management. The principles are also correlated with the risk management framework and the risk management processes related to each other [9]. Principles that are not applied will eliminate the basic pillars of the standards adopted as shown in Figure 1 below.

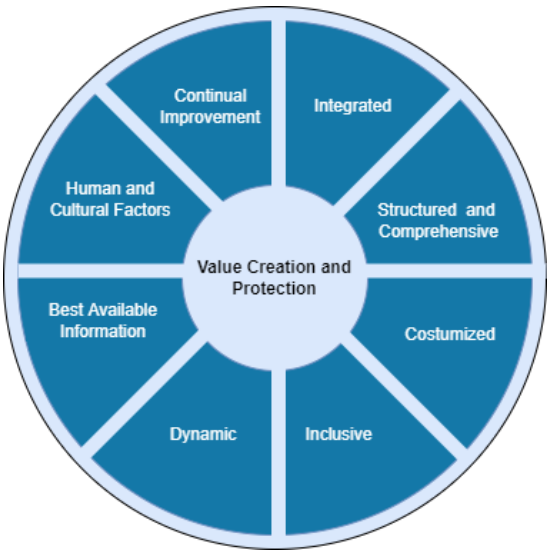

Figure 1. Principles of Risk Management

Based on Figure 1 there are 8 (eight) principles that must be carried out as followers :

1. Integrated, risk management is part of integrated organizational activity.
2. A structured and comprehensive, structured and comprehensive approach, the results are comparable and consistent
3. Adapting to user needs, the framework and management processes are tailored to the needs of the organization and are in line with the internal and external context and defined objectives.
4. Inclusive, involving stakeholders adequately and following the implementation time, will make the related parties willing to open their views, high awareness, and perceptions to be taken into consideration in the risk management process and mature.
5. Dynamic, risks that arise or disappear can change the external and internal context. Risk management will anticipate, scan and understand, and adequately deal with changes that occur.
6. The best information available, risk management input is based on historical and current information, as well as future expectations.
7. Human and cultural factors, Human behavior, and culture significantly influence all aspects of risk management at every level and stage.
8. Continuous repair,risk management is improved continuously or continuously based on learning and experience.

2.6 Framework of Risk Management

The framework provides organizational procedures and arrangements that will implement risk management at all levels of the organization. every organization should have a policy or strategy to decide when and how risk management is carried out and how to handle it [9]. The framework is not intended to describe a system, but to assist organizations in integrating risk management into the overall management system. as well as the organization can adapt the components of the framework to suit the needs of the organization. The framework used in risk management SNI ISO 31000:2018 is similar to the method that has been popularly used in management science, namely, the PDCA (Plan, Do, Check, Action) method popularized by W. Edwards. As for the PDCA Cycle, ISO then formulates a risk management framework with a repeating pattern and there are 5 activities in it as shown in figure 2 [9].

Figure 2. Risk Management Framework

Based on Figure 2 there are 6 (six) components of the framework as follows :

1. Leadership and Commitment, are associated with the organization where the top management of supervisors, ensure that risk management activities are well integrated, and adjust all components of the framework and their implementation.
2. Integration, risk management also depends on understanding the organizational context and its structure. Every company or organization has a different structure and it also affects the context of the goals, objectives of the organization.
3. Desain, when designing a risk management framework, the organization should be able to understand the external and internal context.
4. Implementation, implemented framework related to planning development including time and resources, identification, modification of decision making as appropriate and where necessary.
5. Evaluation, the effectiveness evaluation will measure the flow of the framework periodically by the objectives, then indicators and behaviors expected from the implementation plan section, and determine the framework so that it remains appropriate to support organizational achievement.
6. Repair, the organization implements continuous improvement and adapts the risk management framework to make external and internal changes, it is done to increase value.

2.7Risk Management Process

Management process clause (vi) is part of the organizational culture, organizational best practices, and business processes organization. The flow chart illustration of the series of activities in the risk management process according to SNI ISO 31000:2018 is shown in Figure 3 [10].

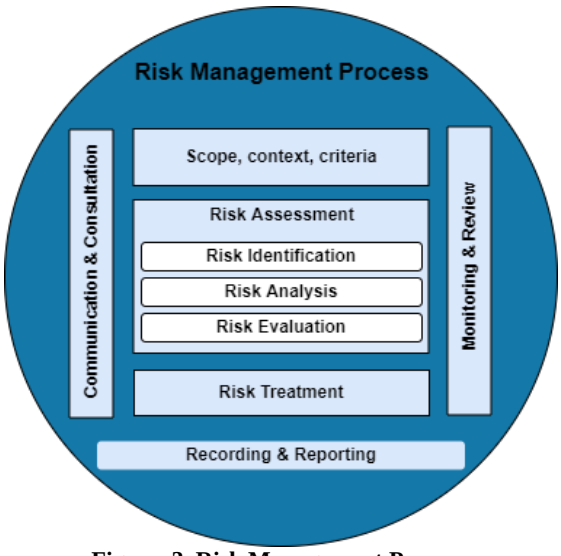

Figure 3. Risk Management Process

1. Communication and Consultation are important at the risk management stage and are expected to create adequate support in making management activities right on target [11].
2. Determining Context, this process occurs in a strategic context and follows a process's goal setting and planning. this is done to determine the basic parameters by which risk must be managed and establish the scope for carrying out the risk management process [12].
3. Risk Assessment, the ISO 31010:2009 standard provides 31 assessment techniques starting from the risk identification stage, risk assessment to the risk evaluation stage according to the type of qualitative, semi-quantitative, or quantitative probability by providing a map or list of application tools that can be used for risk assessment. The application of the method is described as highly applicable (Strongly Applicable/SA), applicable (Aplicable/A), and not applicable (Not Applicable/NA).There are 3 things to identify :
   a. Risk Identification, risk analysis is an important aspect of risk management by listing as many risks as possible [13]. This risk identification process is important to be carried out extensively and this risk identification is also carried out on risk and outside the control of the organization [14].
   b. Risk Analysis will be used as input for risk evaluation and can be used for the decision-making process regarding risk treatment. This risk analysis refers to two parts of risk, namely impact, and probability [15]. The scale and combination method used must be consistent with the previously established risk criteria [16].
   c. Risk Evaluation in the risk evaluation process, it will be determined which risks require treatment and how to prioritize these risks. The results of the risk evaluation will be input for the risk treatment process [17].
4. Risk Treatment, define risk treatment as a process to modify risk. then apply those options. Risk treatment is an iterative process, starting from assessing a risk treatment to estimating whether the remaining risk level is acceptable, according to the established criteria. Identification of risks where the stages that determine suggestions and treatment for all possible risks that occur and are expected to minimize the possible risks that exist [18]. Risk treatment is an activity that takes actions to minimize risks to the system and chooses risk implementation options and takes into account the perceptions of stakeholders 19].
5. Monitoring and Review are carried out regularly, there is a reduction in risks and impacts caused and activities are carried out with meetings to discuss obstacles or possible disturbing risks, this application also exists in research by making communication and consultation plans as well as compiling RACI Matrix [20].The implementation of the review should be carried out at all stages of the process which includes planning, gathering information analysis, and recording results [21].
6. Reporting and Recording, the owner receives reports from the contractors and supervisory consultants regarding problems in the field or the suitability of the work that has been done. whether the implementation is appropriate [22]. The correlation of these stages is the final reporting stage of the risk assessment that has been listed in the communication and consultation plan and the agency validates the formulation of the results [23].Reporting becomes an integral part of organizational governance and becomes a dialogue between stakeholders and supports the risk management process [24]. Documented guidelines

will assist in an effective and efficient monitoring process. Recording and reporting of the risk management process can be developed independently in the form of a report approach that is by the organizational context. The recording and reporting method applied is the operational risk report method which is presented in the form of a table containing many variations of data [25].

3. METHODOLOGY

3.1Research Stage

Researchers carry out several stages as a basic framework so such as the research stages in figure 4.

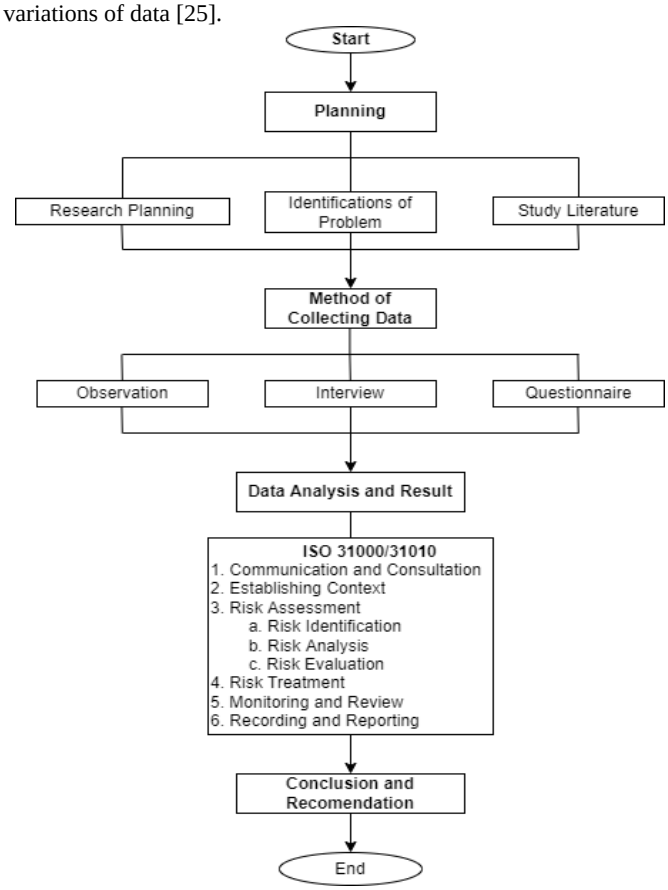

Figure 4. Research of Stage

At the planning stage, the researcher carried out several plans, namely:

1. Determine what topics, will be used as research material. The topic used is LMS (Learning Management System) service risk assessment. Determine what method will be used in the research. The method used is ISO 31000:2018/31010:2009. Determine what object is the research material. The object of this research is LMS (Learning Management System) E-Learning Ahmad Dahlan University Yogyakarta.
2. Identify the problem,s found in the specified object. Observations about what problems can be raised in research and take an outline of the problem to determine that the problem can be solved with certain topics and methods. After knowing then synchronized with topics and methods to analyze the problem further.
3. This stage searches for books, articles, previous research, and journals related to the topics and methods chosen as references and research literacy.

3.2Method of Collecting Data

1. Observations are carried out at the research stage to observe and review an object to be studied based on the standard method used. Observation can increase understanding of the working system of an object and researchers can adjust the problems that have been identified with the method used.
2. Interview, qualitative research does not aim to generalize to the population, so the data needed is not related to the sample and population in this study. The results of interviews from these informants can be research subjects who can provide information related to the phenomena or problems raised in this study. Informants in the risk management assessment are divided into three, namely main informants, key informants, and supporting informants. The initial interview was conducted via WhatsApp due to the COVID-19 pandemic.
3. The study made a list of questions by creating a questionnaire that would be distributed to the UAD E-Learning management institution. The questionnaire will use the Linkert model which has a number range from 1 to 5 and the risk variables that have been compiled are then validated by the main informants by combining the probability and consequence values to determine the level of risk that will be categorized at several levels to determine risk priorities.

3.3 Implementation

The risk management assessment in e-learning services is carried out through 6 stages using the ISO 31000/31010 standard.

3.3.1 Communication and Consultation

Communication and consultation with internal and external stakeholders must be carried out as widely as needed and in every application of risk management. The following is a table of communication and consultation planning and the preparation of the RACI Matrix

Table 1. Communication and Consultation Planning

Activity	Con-tent	Purpose	Location	Date
Determination of research implementation	Date & Location options	Setting a date for risk assessment	BSI and LPP-2I	30/09/2021
Implementation of risk assessment	Approaches and Methodologies and risk identification techniques	Early identification 1. Business process 2. Risk Identification 3. Organizational structure 4. Asset Identification 5. RACI Matrix	BSI LPP-2I WhatsApp FTI	30/09/2021 13/10/2021 28/12/2021 14/01/2022 20/01/2022 26/01/2022
Formulation of results	Risk identification results	The results of the assessment from the researcher get an acc from the agency 1. Result of risk evaluation	WhatsApp	05/01/2022
Result reporting	The results of the research	The results of research that have been completed and by applicable regulations 1. Final result document	LPP-2I	10/01/2022

Based on table 1, the risk assessment in this study was carried out in a blinded manner, namely face-to-face and online meetings via WhatsApp to discuss the stages of the assessment. Stakeholders can make plans by including activities and dates for risk management.

Table 2. RACI Matriks

No	Stages of the Risk Management Process	Chancellor	BSI	LPP	PJJ	Infra-structure
1.	Communication and Consulting		C	I	R	C
2.	Define Context		C	I	R	C
3.	Risk Assessment a. Risk Identification b. Risk Analysis c. Risk Evaluation		R C C/A	I	R/A R/A R/A	R/A R/A R/A
4.	Risk Treatment		C	I	R/A	R/A
5.	Risk Monitoring and Review	I	C	I	R/A	R/A
6.	Recording and Reporting	I	C	I	R/A	

The RACI matrix in table 4 outlines how communication is carried out by knowing the letters that are the duties and responsibilities of each party to take action and make decisions. The data generated from the RACI matrix is then used as a guideline for the implementation of the risk management process.The RACI matrix describes the roles and responsibilities of each stakeholder. Determination of the mixed matrix is done by analyzing the organizational structure and interviewing key informants and the results from table 2 there are 4 stakeholders where the chancellor and LPP (educational development institutions) as informed parties are notified about the work on risk management activities and the required resource requirements, while BSI (Information Systems Bureau) and head of an infrastructure as responsible, namely those who carry out risk management, accountable who ensure the work is carried out properly and consulted as parties who provide advice on what treatment is given. and PJJ (distance learning) as responsible and accountable.

3.3.2Establishing Context

The context of the risk management process includes the organization's objectives, scope, or other areas where risk management is applied. Setting the context will be taken into consideration in risk management for the next process. Understanding the scope, external and internal context helps approach the risk management process.

a. Scope, where risk management determinesthe scope of goals and objectives as well as organizational targets by looking at the vision and mission also conducted interviews with informants to equalize perceptions.
b. Context the external context can be determined by describing stakeholder mapping showing the involvement of stakeholders.The internal context determines the taxonomy in which the risk assessment is carried out.
c. Criteria Likelihood & Impact, determination of likelihood adjusted to the tastes of the organization, adjustments are made by having discussions with the process owner by determining the scale of risk events. The impact contains the type of impact received by the risk that occurs and the level of impact that becomes an indicator in measuring the level of risk. For this reason, the impact assessment will also be a reference for research to consider in determining recommendations made by providing a probability scale for each risk variable.

3.3.3Risk Assessment

The risk assessment has 3 structural elements that are the stages of the assessment, namely risk identification, risk assessment, and risk evaluation. research methods ISO has published technical guidelines on how to assess risk and ISO 31000:2018 has a complementary standard for the assessment stages, namely ISO 31010:2009 management risk assessment techniques.

3.3.3.1 Risk Identification

Asset Identification the asset identification stage is carried out by interviewing key informants and key informants, both informants who provide information or expert judgment.

Table 3. Identification of Assets

Identification of E-Learning Assets	
Data	A data report from each study program
Software	1. MySQL version 5.10 2. LMS Moodle 3.8.9 3. PHP version 7 4. Web server engine-x
Hardware	1. Servers 3 pieces 2. RUN 16 x 3 3. CPU 4 x 3 4. Storage 1 TB

Identification of risk possibilities and impact information is obtained by the what if method or checklist accompanied by a brainstorming approach, then each event that will cause unwanted consequences is formulated.

Table 4. Identification of Possibilities and Impact

Source of Risk	ID	Possibl Risks	Impact
Natural of Environmental	KR01	Earthquake	Damage to infrastructure assets and can stop business activities
	KR02	Flood	Damage to infrastructure assets and hampered activities,
	KR03	Lightning	Damage to infrastructure assets and disrupted business processes
	KR04	Fire	Loss of infrastructure assets and suffer financial loss
	KR05	Dust or dirt	Damage to equipment that will overheat
Human	KR06	Device theft	Financial loss, data loss
	KR07	Misuse of access rights or user ID	Getting cyber threats, theft of company data and information
	KR08	Human error	Organization experiencing difficulties, operational process disruption
	KR09	Data information does not match facts	The occurrence of data manipulation that disrupts business processes
	KR10	Cybercrime	Corporate losses, data theft
	KR11	Leakage of internal data or information	Loss of public trust, reputation,

			law, fines
	KR12	ResignationEmployees	Operational management activities are hampered
	KR13	do not follow all SOPs	Business processes are not running well, changing company conditions
	KR14	physical access and maintenance	Physical identity fraud and misuse of
	KR15	Network system failure or network disconnects	Unable to share data, damage to network cables and connectors, and cannot access the main program
System and Infrasructure	KR16	or damage failure	Interfere with operational activities, unable to update, vulnerable to malware viruses, functions do not run optimally
	KR17	or damage failure	Data loss, financial loss, operational activities interrupted
	KR18	Failure update failure	Can cause
	KR19	Disk error or disk full	Resulting in system slowdown, corrupted files, blue screen
	KR20	Data corrupt Data	, data loss, business processes disrupted
	KR21	Database Overload	Impaired performance, access slows down cannot be accessed
	KR22	Server is down	by hacker attacks that
			can disrupt the website
	KR23	Overheating of computer equipment	Causes overheating and cause self-death
	KR24	virus attack Malware	Changes the appearance of the website, annoying malware, hackers access to the website
	KR25	System Crash	Log error, hinder operational activities
	KR26	Backup failure	Loss of data and cannot be accessed again, detrimental to
	KR27	Outdated technology	Quality capacity cannot accommodate operational needs, hampers business activities, is not optimal in program management
	KR28	Server short circuit due to electricity	Infrastructure damage hampers operational activities
	KR29	Program anomaly appears which cannot be above the program	Loss of data, hampering operational

Based on table 4, the possible risks are classified based on the source of the risk, sources caused by nature or the environment have 5 possibilities, to the sources of risk caused by humans have 9 lists of possible risks, and sources of risk caused by possible risks that have been previously identified occur in the operational system. The description of this impact will be a consideration for how to provide treatment or treatment that must be carried out on the risks that occur.

3.3.3.2Risk Analysis

Stages of risk analysis are conducting a rating which is decided based on two aspects of likelihood and impacts.The risk analysis stage will be an evaluation in the decision-making process regarding the treatment of risk. In the previous stage, namely determining the context of the

formulation of the likelihood and impact criteria, it will determine the risk assessment. The analysis is carried out with an approach to obtain information related to the level of risk carried out with key informants who manage business processes. The value criteria that become the assessment indicators based on the frequency of occurrence and their descriptions can be seen in table 5.

Table 5.Criteria ValueLikehood

Value	Frequency	Description	Criteria
1	1 time in a year	Almost impossible	Rare
2	1-2 times in one year	likely to occur	Unlikely
3	3-4 times a year	Likely to happen and not happen equally	Possible
4	4-5 times a year	Most likely to happen	Likely
5	>5 times in a year	Almost	Likelihood

Criteria certain determined based on numbers that have been categorized according to the frequency of occurrence and which will be validated from the answers of the informants.

Table 6. Criteria Value Impact

Value	Criteria	Impact
1	*Insignificant*	Does not affect the process
2	*Minor*	Only has a very small impact on not achieving the targets and performance targets can still be achieved
3	*Moderate*	Delay in achieving goals is quite large and performance achievement below target
4	*Major*	Delay in achieving goals is very significant and achievement performance is far below target
5	*Catastrophic*	Failure to achieve targets and failure to achieve work

Based on table 6, Impact variables have also been validated with a scale and 1 and 2 on impact, also show numbers where the impact that affects the system does not have a large impact.

3.3.3.3Risk Evaluation

Based on table 7, the consequence/probability matrix shows 3 colors that describe the level of the risk. The rating scale shows a value of 1 1 with a total of 13 risks, which means the risk is at a low level. The risk code in the matrix in the second criterion is unlikely, i.e. the possibility of a risk occurring is small and the second is Minor. The risk that occurs has a very small impact and the process can still run with a value of 2 2 with a total of 16 risks being at a low level.

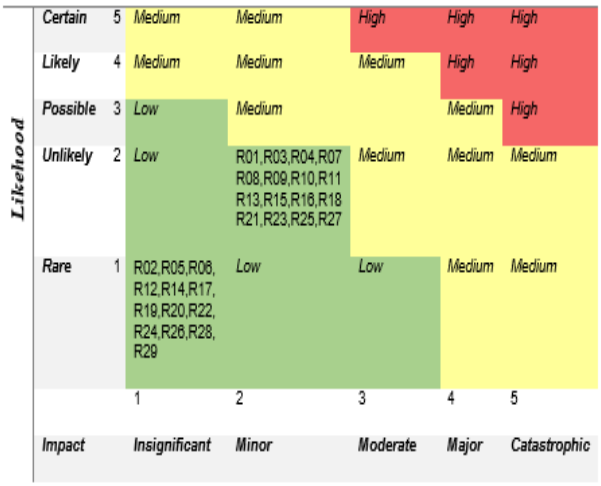

Figure 5. Evaluation of Probabilities/Consequence Matriks

3.3.4Risk Treatment

Risk treatment is an activity that takes actions to minimize risks to the system and chooses risk implementation options and takes into account the perceptions of stakeholders. Risk treatment involves several things, namely the formulation and options of risk treatment, planning and implementation of risk, and making a decision whether the risk is acceptable. Risk treatment is determined by the value of the probability and consequences of problems that are categorized into four, namely:

a. Risk Retention (Retention), by dividing the risk that needs to be handled by a party and not causing too big a loss [20].
b. Risk Reduction (Reduce/reduce), by carrying out activities or reducing the consequences of risk by changing methods, or implementing processes [20].
c. Risk Transfer (transfer or sharing), by sharing risk with other parties or using other options to reduce the impact that occurs [20].
d. Risk Avoidance (Avoiding), cannot be controlled and has very large consequences so that risk must be avoided. [20].

The mapping of risk treatment can be seen in table 7 as follows.

Table 7. Risk Treatment

ID	Possible Risk	Risk Treatment Criteria Risk	Treatment
R01	Earthquake	Reduction	backup infrastructure provision hardware and mirroring database for backup.
R02	Flood	Retention	backup infrastructure provision hardware and mirroring database for backup.
R03	Lightning	Reduction	backup infrastructure provision hardware and mirroring

			database for backup.
R04	Fire	Reduction	backup infrastructure provision hardware and mirroring database for backup. Prepare fire extinguishers (APAR) in the building
R05	Dust or dirt	Retention	Check and clean devices regularly to avoid damage
R06	Theft of	Retention	Provide CCTV to control devices and improve security guard
R07	Misuse of access rights or user ID	Reduction	Change passwords and usernames periodically
R08	Human error	Reduction	Provides an understanding of system handling and management following SOPs, provides direction and periodic evaluation
R09	Information data does not match facts	Reduction	Gives high access rights to the person in charge and performs verification before managing data information
R10	Cybercrime	Reduction	Protects data with high-security software and antivirus installation for website
R11	Leakage of internal data or information	Reduction	Provide direction and monitoring and make agreements with stakeholders with management and include sans legal action by applicable organizational provisions
R12	Resignation	Retention	Prepare routine employee evaluations by paying attention to employee skills
R13	Employees do not follow the entire SOP	Reduction	Conduct intense communication and consultation regarding the enforced SOP by providing direction and guidance
R14	Physical access and maintenance are not	Retention	Perform periodic maintenance and checks to minimize damage to
	terotorisasi		infrastructure
R15	Network system failure or network disconnected	Reduction	Perform periodic checks and provide service providers and add a signal booster router so that the system can be accessed
R16	Software failure or damage	Reduction	Perform software updates, reinstall and install anti-virus to avoid malware
R17	Hardware failure or damage	Retention	Assessing appropriate and quality hardware specifications and providing hardware backup
R18	Update failure	Reduction	Checking storage space, checking device manager, and clearing system cache
R19	Disk error atau disk full	Retention	Adding a hard disk storage backup according to the required capacity
R20	Data corrupt	Retention	Anticipating by checking regularly and backing up the main data
R21	Overload database	Reduction	Perform periodic monitoring of DB log, CPU usage, RAM usage and main database
R22	Server down	Retention	Perform regular checks on the main database and refresh the log, temp, and RAM
R23	Computer device overheating	Reduction	Provide sufficient air conditioning so that the device does not overheat
R24	Malware virus attack	Retention	Install antivirus and update if there is an update as well as monitoring software and database
R25	System crash	Reduction	Perform system repairs and maintenance on a regular basis
R26	Backup failure	Retention	Check the usage of storage memory used to prevent the emergence of viruses/malware
R27	Outdated technology	Reduction	Checking and recording device usage, and usage time, and carrying out routine

			maintenance so that the device can last a long time
R28	Server short circuit due to electricity	Retention	Checking the condition of electrical cables, making sure the electrical conductors are closed and consulting directly with electrical installation services
R29	A program anomaly appears that the program cannot access	Retention	Overcome anomalies by creating new support programs and consulting with expert technicians for further repairs

The risk treatment described in table 13 above is carried out for control efforts carried out to reduce risk events. the determination of risk treatment is carried out through consultation and communication and reference analysis with the system manager so that treatment decisions cannot be separated from the manager's perception and can be applied by organizational provisions.

3.3.5 Monitoring and Review

All activities or any changes in the assessment can be identified with a validated risk list from the parties concerned and communicating and consulting.

3.3.6 Recording and Reporting

Recording and reporting of the risk management process can be developed independently in the form of a report approach that is by the organizational context. The recording and reporting method applied is the operational risk report method which is presented in the form of a table containing many variations of data.

4. CONCLUSION

Based on the results of the analysis and discussion that has been carried out, the conclusions that can be drawn are the risk assessment of the Ahmad Dahlan University E-Learning LMS (Learning Management System) service using ISO 31000:2018/31010 carried out by determining risk identification based on risks that have occurred, that occurred current and future risks, by conducting a risk assessment using a probability and consequence matrix that is validated from the expert judgment of key informants as well as determining the level of risk or risk level and providing recommendations for risk treatment that occurs. The risk assessment of 29 variables occupies 2 categories of the same risk level but in different categories, namely, 13 risk variables at a low level with a probability consequence number of 1 1 (Rare-Insignificant), and 16 risk variables at a low level with a probability/consequence number 2 2 (Unlikely-Minor). Risk treatment is based on the result of the evaluation of the risk level that has been determined with the results of 13 risk variables in the risk retention category and 16 risk variables in the risk reduction category. In the entire process of managing the e-learning system and server, the implementation of the risk management process has not covered all stages of ISO 31000:2018/31010 standard assessment..

5. REFERENCES

[1] N. Terry George Abisay, "Risk Management at Soekarno Hatta Airport Based on ISO 31000," pp. 116 - 129, 2013.

[2] Lalonde, C., & Boiral, O. (2012). "Managing risks through ISO 31000: A critical analysis. Risk Management, 14(4), 272–300.

[3] Susilo Leo J. and Victor Riwu Kaho 2018. "ISO 31000:2018-Based Risk Management: A Guide for Risk Leaders and Risk Practitioners.". Jakarta: Gramedia Widiasarana Indonesia.

[4] Agustinus, Stefan., Nugroho, Adi., Cahyono, Ariya Dwika. (2017). "Information Technology Risk Analysis Using ISO 31000 in HRMS Programs.," vol.1.

[5] Castells, Manuel & Cardoso, Gustavo, eds. 2005. The Network Society: From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations.

[6] McFadden, dkk. 1999. Database Concepts and Practical Guide. Yogyakarta.

[7] Indriantoro. "The Effect of Computer Anxiety on Lecturer Skills in the use of Computers," Indonesian Journal of Accounting and Auditing, Vol. 4, 2000.

[8] SNI IEC/ISO 31000:2009. 2011. "Risk Management – Principles and Guidelines". National Standardization Agency. Jakarta.

[9] ISO 31000:2018. "Risk Management – Guidelines (ISO 31000:2018)". BSI Standards Limited 2018. Switzerland.

[10] SNI IEC/ISO 31010:2009. 2016. "Risk Management – Risk Assessment Techniques". National Standardization Agency. Jakarta.

[11] Lisananda, Aldesra Azria. (2021). "Construction Risk Management in Wastewater Piping Construction Projects Based on ISO 31000:2018 Concepts." Essay. Yogyakarta: Indonesian Islamic University.

[12] Putra, Muhammad Nofeliansyah. (2019). "Analysis of ISO 31000-Based Academic Information System Technology Risk Management (Case Study: UIN Sunan Kalijaga). Essay. Yogyakarta: UIN Sunan Kalijaga.

[13] Miftakhatum, (2020). "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," vol.1..

[14] Woody, Carol. "Applying OCTAVE: Practitioners Report," Carnegie Melon University. 2006. US.

[15] Sukri, Muh. (2020). "Risk Management Analysis on Administration System using OCTAVE Allegro Framework".

[16] Alvian, Fawwaz Afif., Sulaiman, Muhammad Haikal et al. (2020). "Risk Management at the Integration Laboratory of the State Islamic University of Sunan Ampel Surabaya using ISO 31000," vol.12.

[17] Setiawan, Ito. Sekarini, A. R., Waluyo, Retno., Alfiana, F. N, "Information System Risk Management Using ISO 31000 and ISO/IEC 21001 Control Standards in Tripio Purwokerto", vol.20, no. 2, pp. 389-396, 2021.

[18] D. D. J. Andi Novia Rilyani. Yanuar Firdaus, "Risk Analysis of Information Technology Based on Risk Management Using ISO 31000 (Case Study: i-Gracias

Telkom University)," e-Proceeding of Engineering, pp. 6201-6208, 2015.).

[19] Kobo, F. N. 2011. "Risk Management Methodology. Enterprise Risk Management Strategy".

[20] Maralis Reni and Triyono Aris. 2019. Risk Management. Yogyakarta: Depublish CV Budi Utama publishing group.

[21] Nice, Francisca Lady and Imbar, Radian Victor. "Information Technology Risk Analysis in Institutions National Aeronautics and Space Agency (LAPAN) on SWIFTS Site using ISO 31000, Vol. 2, No. 2, pp. 2-3. 2016.

[22] Innocent, Robin. 2018. "ISO 31000-Based Risk Management Analysis on Company Operational Aspects (Case Study: Cafe Industry, Sleman Regency, DIY). Essay. Yogyakarta: Sanata Dharma University.

[23] De Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. 2017. The ISO 31000 standard in supply chain risk management. Journal of Cleaner Production, 151(March), 616–633.

[24] Labombang, M. 2011. "Manajemen Risiko dalam Proyek Konstruksi". Jurnal SMARTekv Vol 9 No 11 Februari 2011. Staf Pengajar Jurusan Teknik Sipil. Fakultas Teknik. Universitas Tadulako. Palu.

[25] Rahmawati, Aprilia., Wijaya, Augustine Fritz. (2019). "Information Technology Risk Analysis using ISO 31000 in ITOP Applications," vol.2.