

# **Analysis of Learning Management System Service Risk Assessment using ITIL V4 Framework**

**Andita Dewi Rinaldi**  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

**Imam Riadi**  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

## **ABSTRACT**

Learning Management System is a distance learning tool that in its management and application uses website-based information technology at Ahmad Dahlan University, which in its application contains a series of learning activities that depend on the system. The risk assessment carried out on the LMS serves to identify potential threats that can occur and prepare appropriate handling steps when incidents and problems occur. In this research, the ITIL 4 framework is used as a guideline for analysis with a research focus on Incident Management and Problem Management practices. Data collection applied in this research is in the form of observations, interviews, and questionnaires. Respondents who will fill out the questionnaire are obtained from the results of the RACI matrix mapping. The data obtained will be analyzed to determine the level of capability of the service and then an analysis is carried out in accordance with the stages of practice contained in incident management and problem management. Based on the results obtained through these stages, a draft Standard Operating Procedure is prepared in accordance with the SOP preparation format used by Ahmad Dahlan University. This research resulted in an assessment of the level of LMS capability in incident management at level 2 in the form of practices that systematically meet objectives using a series of basic activities, for problem management at level 1 in the form of practices that are not well organized. This research provides a draft SOP (Standard Operational Procedure) in accordance with ITIL 4 guidelines which results in 6 additional forms in 14 activities.

## **Keywords**

ITIL 4, Incident Management, Problem Management, Standard Operating Procedure, Learning Management System

## **1. INTRODUCTION**

Importance of higher education as an educational institution as an institution that serves the community, it is an obligation for universities to maintain the quality of their services so that the community continues to make higher education the main choice in pursuing education. [1] Learning Management System is the development of plans and implementation of independent learning under the auspices of the Educational Development Institute (LPP). LMS (Learning Management System) is software that can deliver learning materials, LMS is an online web-based multimedia resource to manage and facilitate learning activities. Universitas Ahmad Dahlan LMS portal was developed to facilitate learning activities when it is not possible to hold face-to-face meetings in class. [2] Based on the rapid development of Universitas Ahmad Dahlan LMS, risk management is needed that can identify risks so that it can help develop strategies that can be managed properly with existing resources.

Risk management is a structured approach to managing threats that may or may not occur in a series of human activities such as risk assessment, strategies for managing those risks and risk actions by managing or optimizing resources [3]. Risk management is needed in the decision-making process when facing various risks that may or have occurred, such as in managing information technology risks, as an assistant in developing business processes that will generate maximum profits and as an effective, efficient and optimal way of managing resources. [4] LMS is a website-based service. Currently, LMS has not implemented guidelines or frameworks that are useful for assessing possible risks or obstacles that have the potential to occur in operational activities so that they can cause the management of LMS services to not be optimal. In this research, the framework used is the Information Technology Infrastructure Library (ITIL). ITIL is a framework that focuses on regularly measuring and improving the quality of IT services provided, both from a business and customer perspective. [5] ITIL is a framework created and developed by the Office of Government Commerce (OGC) in the UK in 1989 [6] The application of ITIL aims to be able to build effective and efficient services for customers, in addition to producing more optimal IT service management and being able to improve the quality of IT services in the direction of periodic service improvements [7]

This research focuses on the Incident Management and Problem Management domain. The selection of this domain is based on the absence of incident and problem handling that has standardized procedures and specific documentation. Incident and problems that occur have an impact on the business processes that run on the LMS. Based on this, the purpose of this research is to determine the level of ability of the LMS in handling events and problems and provide a successful design of Standard Operating Procedures (SOP) to handle problems that may occur at the Universitas Ahmad Dahlan LMS. In addition, one of the objectives of the ITIL framework is to improve the operational efficiency of IT institutions, improve service quality standards, improve the effectiveness and efficiency of service delivery. [8]

## **2. LITERATURE STUDY**

### **2.1 Understanding of assessment**

Assessment is the process of collecting accurate data about the level of achievement of objectives. This data is then used to provide feedback, evaluate outcomes, and make decisions about teaching and program development and effectiveness. [9] Assessment is an ongoing process that involves collecting, using and interpreting valid evidence of what has been achieved to make decisions about how the system is working. [10] Broadly speaking, assessment is a process of judging, measuring, or assessing something that aims to provide information that can be used for decision-making or improvement. The assessment process involves collecting data,

analyzing, and interpreting relevant information to make judgments or conclusions.

## 2.2 Understanding of risk

Risk is uncertainty or unpredictability that can lead to loss. Information technology risk is a company that uses or implements information technology and then has the possibility of a risk occurring. Company operations and the existence of new challenges in achieving strategic goals and objectives are something that can be affected by information technology risks. [11]

## 2.3 Risk Identification and Assessment

Risk identification is an activity related to the collection of all information about a business, which will then be analyzed to find all possible risks that can cause losses. Conducting risk identification is useful for knowing all the risks that may be faced by business stakeholders, which in the future business people will be faced with many risks, ranging from small risks to large and broad risks. [12]

## 2.4 Kinds of Risk Management

Risks can generally be categorized into:

1. Speculative Risk  
A risk that has two possibilities, namely the possibility of loss or the possibility of profit, is the definition of speculative risk.
2. Pure Risk  
A risk that has only one possibility, namely the possibility of loss. [13]

## 2.5 ITIL Method

ITIL is a framework developed since 1980 as a guideline for organizations or companies by the UK Government Office of Trade. The world recognized ITIL as the de facto standard in the field of service management in the mid-1990s. In February 2019, ITIL 4 was released in stages in the following months. as a form of renewal of ITIL to respond to the growing development of ITSM. The implementation of the ITIL framework provides a detailed overview of several essential IT practices with comprehensive and customizable checklists, checks, tasks and procedures for all types of IT organizations as shown in Figure 1. [14] ITIL 4 builds on more established ITSM practices in a broader context, where ITIL 4 consists of 34 practices. In this research, the ITIL 4 practices used come from service management with the practice of incident management and problem management.

ITIL has core components, namely the Service Value System (SVS) and the four-dimensional model. ITIL SVS describes how to create value through all components and sets of organizational activities that work together. The purpose of SVS is to ensure that the organization continues to create value together with all stakeholders through the use and management of products and services. The left side of the figure shows the opportunities and demands that come to the SVS from both internal and external sources. The right side shows the value created for the organization, its customers, and other stakeholders. [15] To ensure a holistic approach to service management, ITIL V4 outlines the dimensions of service management, where each SVS component must consider four dimensions, namely organization and people, information and technology, partners and suppliers, value streams and processes as shown in Figure 2.

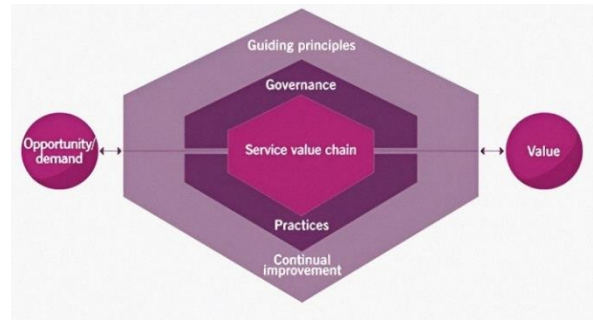


Figure 1. Structure ITIL 4

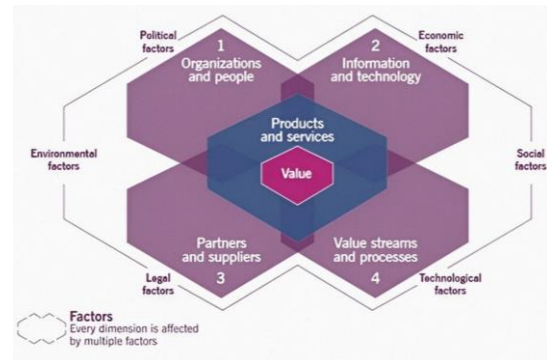


Figure 2. The Four Dimensions ITIL 4

There is also an SVS element, namely the service value chain which is a series of interconnected activities within an organization to produce services that are of value to consumers and facilitate value realization. The service value chain as shown in Figure 3

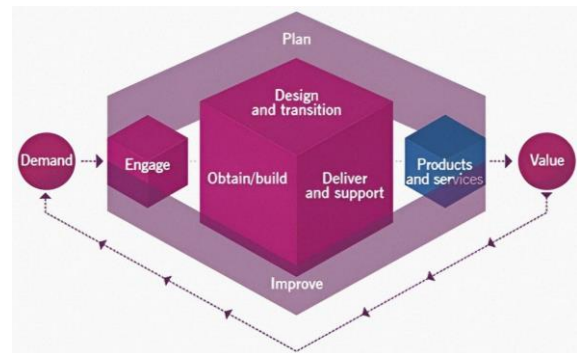


Figure 3. Service Value Chain

In this research, the ITIL 4 practices used are incident management and problem management, which in each practice have stages that are used to handle events or problems that occur. Incident Management has 7 steps while for problem management there are 3 steps. [16] as show in Figure 4 and Figure 5

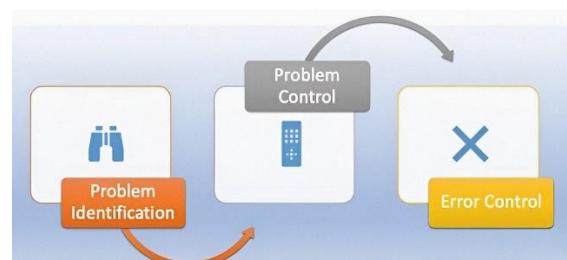


Figure 4. Problem Management Steps ITIL 4

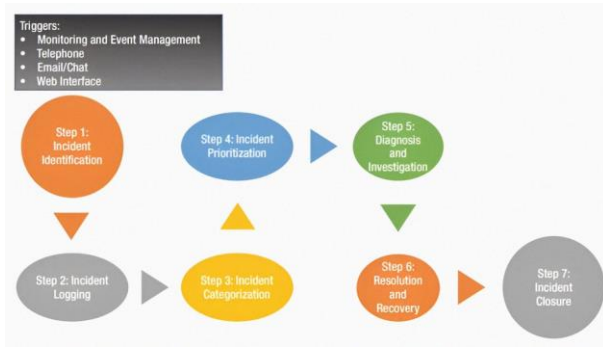


Figure 5. Incident Management Steps ITIL 4

## 2.6 Learning Management System

Learning Management System (LMS) is software used for administration, documentation, validation, reporting, online learning and distance learning activities using electronic media connected to the internet, intranet or other computer media and contains modules or learning materials. [17] Universitas Ahmad Dahlan LMS is used for web-based online learning process. This system can be reached using a PC, laptop or smartphone connected to the internet network. This system was built to answer learning challenges that are limited by time and space, learning media and learning resources. The success of learning objectives is due to the independence, cooperation, active participation and trust between lecturers, students and the community. [18]

## 2.7 SOP (Standard Operating Procedure)

In general, the SOP serves to regulate the duties and functions of each element (implementer) in carrying out its role in the type of activity that involves more than one work unit / field of work. Therefore, SOP is a document related to procedures or steps that will be carried out chronologically for a job in order to get maximum work results [19] There are several types of SOPs, one of which is SOP according to the Scope and Type of Activity which is categorized into two types, namely general SOP and specific SOP. This type of SOP is distinguished by the nature and content of activities and stages of implementation. SOPs have several formats, namely simple steps, sequential stages, graphs and flow charts whose use is adjusted to the objectives to be achieved by the organization. [20]

## 3. METHODOLOGY

This research has several stages in its implementation to collect the data needed for the analysis process. These stages are as follows:

1. Observation  
Observation is a way of collecting data by observing and studying an object to be studied based on the method to be used. [21] In this research, this process will be carried out directly at Universitas Ahmad Dahlan Yogyakarta to observe and see what problems and incident occur during the implementation process.
2. Interview  
Interview is a data collection technique that is carried out face-to-face and asks several questions directly to related parties. [22] In this study the interviewees were LMS management staff and Information Systems Bureau staff.
3. Questionnaire

The questionnaire is a data or information collection technique that can be used to analyze the characteristics, behavior, beliefs and attitudes of a number of key people in an organization. In this study, the questionnaires to be distributed are arranged based on the adjustment of the stages in each practice which are then distributed to respondents to be filled in. Respondents in this study were selected based on the RACI diagram mapping.

### 4. RACI Chart

The RACI diagram is a matrix of all activities or decision authorizations that must be taken in an organization related to all parties or positions involved. The RACI diagram contains a number of organizational structures that describe roles and responsibilities. [23] RACI stands for Responsible, Accountable, Consulted, Informed. [24]

## 4. RESULTS AND DISCUSSION

In this research, the analysis and discussion stage begins after data collection in the section determining the level of capability of the UAD LMS after determining the analysis will continue to analyze in accordance with the ITIL 4 practices used, namely incident management and problem management with predetermined stages. Based on these stages, the results of the SOP design are compiled in accordance with the format that has been standardized and applied by Ahmad Dahlan University which can be applied in handling incident management and problem management.

### 4.1 Capability Model ITIL 4

The selected practice skills assessment is one of the three assessment approaches that can be used to seek maturity analysis in ITIL 4. The selected practice skills assessment only assesses the capabilities of one or more selected practices with unassessed SVS maturity. In this study, this approach was used according to the number of practices performed, namely incident management and problem management. At the capability level there is a scale that applies to each management practice, including the following:

1. Level 1, disorganized practice
2. Level 2, a practice that systematically fulfills its objectives by using a set of basic activities and supported by specific resources.
3. Level 3 a practice that is well defined and achieves its goals in an organized manner, using specific resources and using other practices incorporated in the service management system for improvement considerations.
4. Level 4 a practice that has achieved its goals in a highly organized manner, the performance of its management system is constantly monitored, measured and assessed.
5. Level 5 a practice has entered the stage of enhancing the capabilities of related organizations

There are 2 PSFs developed in this study for incident management and 1 PSF developed for problem management. [25] Level of ability is obtained from the results of interviews and questionnaire analysis based on the criteria compiled. then the results are obtained as shown in Table 1.

seen in Table 2.

**Table 1. Capability Level LMS**

Incident Management			
PSFs	Capability Criteria	Dimension	Capability level
Ensuring identification in overcoming and reducing impact of incidents is carried out optimally	Identification and recording procedures have been adapted from a relevant standard to handling incidents	Value streams and Process	2
	Responsibilities for identifying and recording are precisely defined	Organization and people	3
	Use of incident logging technology applied to the service	Information and technology	2
Ensuring operation of LMS services that are stable and responsive to incidents that occur	Duration of incident handling.	Value streams and Process	3
	Consultation and communication between teams for handling incidents.	Organization and People	3
	Facilities from third parties that can support the effectiveness.	Partner and supplier	3
Problem Management			
PSFs	Capability Criteria	Dimension	Capability level
Ensuring that problem prevention and handling are carried out optimally	Analysis and evaluation of root causes to prevent recurring problems.	Value streams and Process	3
	Procedures for recording and documenting problems.	Value streams and Process	1
	Handling coordination that has been agreed with the team concerned	Organization and people	3
	Monitor and evaluate the effectiveness of the steps	Value streams and Process	3

The overall proficiency level of a practice is determined by the highest level that meets all proficiency criteria. So in the research conducted, the results were found in the form of incident management from 2 PSFs with 11 criteria, the results showed that the level of ability was at level 2 while for problem management from 1 PSF with 4 criteria, the results were in the form of a level of ability that was at level 1 which indicated that in the LMS.

## 4.2 Incident management

Based on the results of interviews, questionnaires and data processing in this study, the results of data analysis are based on the stages of incident management which include 7 steps

### Incident identification

In the process of identifying events that have occurred in the LMS will be carried out with a brainstorming approach resulting from the acquisition of interview results which can be

**Table 2. Incident Identification LMS**

Source Incident	ID	Incident or possibility incident
Natural	IK 1	Earthquake
	IK 2	Fire
Human	IK 3	Abuse right access or user ID
	IK 4	Human error
	IK 5	Information Data no in accordance
	IK 6	Cybercrime
	IK 7	Failure or damage soft and hard device
	IK 8	Disk Error or disk full
	IK 9	Server Down
	IK 10	Database Overload
	IK 11	Virus or malware attack
	IK 12	Technology Worn

Identification of events that can occur on the LMS is grouped into 3 sources incident, with the results of sources from nature having 2 possibilities or events that can cause damage to the LMS, then sources of events originating from humans have 5 possibilities or events, and finally sources of events originating from systems and infrastructure have 10 possibilities of events or events on the LMS.

### 4.2.1 Incident recording

Incident recording stage is the stage where all identified events must be recorded with a clear and unchangeable timestamp. However, this has not been applied to e-learning so that the results that can be displayed in the form of information on whether or not the incident occurs frequently, can be seen in Table 3.

**Table 3. Incident Recording LMS**

ID	Incident or possibility incident	Frequency it happened incident
IK 1	Earthquake	1-2 times in 1 year
IK 2	Fire	≤ 1 time in 1 year
IK 3	Abuse right access or user ID	1-2 times in 1 year
IK 4	Human error	4 - 5 times in 1 year
IK 5	Information Data no in accordance	1-2 times in 1 year
IK 6	Cybercrime	1-2 times in 1 year
IK 7	Failure system or unstable network	1-2 times in 1 year
IK 8	Disk Error or disk full	1-2 times in 1 year
IK 9	Server Down	1-2 times in 1 year
IK 10	Database Overload	≤ 1 time in 1 year
IK 11	Virus or malware attack	≤ 1 time in 1 year
IK 12	Technology Worn	1-2 times in 1 year

Based on the results of the recording of incident, the most frequent thing that happens is in the form of human error

#### 4.2.2 Incident categorization

At the incident categorization stage, the categorization process of events or possible events that occur, are in need of proper handling and are handled properly as needed, can be seen in Table 4.

**Table 4. Incident categorizing on LMS**

ID	Incident or possibility incident	Category Handling
IK 1	Earthquake	Natural mitigation disaster
IK 2	Fire	Natural mitigation disaster
IK 3	Abuse right access or user ID	Security team <i>cyber</i>
IK 4	Human error	<i>Service desk</i>
IK 5	Information data not accurate	<i>Service desk</i>
IK 6	Cybercrime	Security team <i>cyber</i>
IK 7	Failure or the damage device soft and hard	Maintenance system
IK 8	Disk Error or disk full	Maintenance system
IK 9	Server Down	Maintenance system
IK 10	Database Overload	Maintenance system
IK 11	Virus or malware attack	Security Team <i>cyber</i>
IK 12	Technology Worn	Maintenance system

Based on the categorization results of events or possible incident on the LMS there are several parties who can be responsible for handling the occurrence of incident.

#### 4.2.3 Incident prioritization

At the incident prioritization stage, an assessment is carried out regarding which events have a high urgency and a big impact so that it becomes an urgent situation can be seen in Table 5.

**Table 5. Incident prioritization on LMS**

ID	Incident or possibility incident	Priority Incident
IK 1	Earthquake	P1
IK 2	Fire	P1
IK 3	Abuse right access or user ID	P1
IK 4	Human error	P1
IK 5	Information not accurate	P2
IK 6	Cybercrime	P1
IK 7	Failure or the damage device soft and hard	P1
IK 8	Disk Error or disk full	P2
IK 9	Server Down	P1
IK 10	Database Overload	P1
IK 11	Virus or malware attack	P1
IK 12	Technology Worn	P3

Based on the results of the interview, it is known that the time determined from BSI for the process of handling events or problems is a maximum of 2 x 24 hours, the determination of the priority scale on the LMS has been implemented but has

not been carried out optimally.

#### 4.2.4 Diagnosis and investigation

At the diagnosis and investigation stage is a prefix for the service desk to find out and understand the symptoms of the incident that occurred and try to provide direction to users to carry out basic problem solving to resolve the incident. can be seen in Table 6.

**Table 6. Diagnose and investigation on LMS**

ID	Incident or possibility incident	Diagnosis and Investigation
IK 1	Earthquake	After happen earthquake do checking on physical assets owned by the LMS
IK 2	Fire	After fire resolved do checking on physical assets owned by the LMS
IK 3	Abuse right access or user ID	Do checking is there are users who use the same ID or do suspicious activity in access the last one can form retrieve data or do data modification
IK 4	Human error	Ensure that user has do correct steps to access.
IK 5	Information Data No in accordance	Ensure the data will be changed Already in accordance with what it should be
IK 6	Cybercrime	Do checking against LMS, observing at a time contact the programmer.
IK 7	Failure or the damage device soft and hard	Check where it happens failure or the damage device soft and hard
IK 8	Disk Error or disk full	Inspect an error occurred on the disk if Still Can accessed
IK 9	Server Down	Do checking How Can the server went down
IK 10	Database Overload	Find cause of data overload
IK 11	Virus or malware attack	Check and find reason happen virus attack
IK 12	Technology Worn	Inspect there is update on moodle

Based on the results of diagnosis and investigation, broadly speaking, examine each incident or possible incident to find resolution and recovery in the next step.

#### 4.2.5 Resolution and recovery

Based on the investigation, a resolution can be applied. For widespread events that can affect many users after the resolution is applied, various tests must be carried out to ensure that the event has been resolved. There is a recovery period or time span used to observe the event and be alerted if an error occurs again. Can be seen in table 7.

**Table 7. Resolution and recovery on LMS**

ID	Incident or possibility incident	Resolution and Recovery
IK 1	Earthquake	Do reporting on physical assets that damage and find alternative while to cover failure service.
IK 2	Fire	Do reporting on physical assets that damage and find alternative while to cover failure service.
IK 3	Abuse right access or user ID	Do existing prevention LMS is implemented in the form of access only limited with 1 account in one session
IK 4	Human error	Do communication to user about their problem.
IK 5	Information data not accurate	Do change the data accordingly with correct information from user
IK 6	Cybercrime	Contact the programmer concerned cybercrime issues
IK 8	Failure soft or hard device	Report failure or damage that occurs device lenient on the part maintenance system to handle soon
IK 9	Disk Error or disk full	Report failure or damage that occurs to the disk on the part maintenance system to handle soon.
IK 10	Server Down	Report failure or damage occurs device lenient on the part maintenance system
IK 11	Database Overload	Report failure or damage that occurs device lenient on the part maintenance system
IK 12	Virus or malware attack	Do existing prevention applied in LMS management
IK 13	Technology Worn	Do update in a way periodically on moodle

After finding a solution to the problems that occur on the LMS, the service desk confirms to the user and periodically monitors after the resolution is applied.

#### 4.2.7 Incident closure

When the incident is resolved, confirmation is generally made with the user before closing the ticket or recording the incident, confirmation is made by the service desk to the user to check the reported incident whether it has been resolved properly or not. However, this process has not been carried out properly on the LMS and the recording system has not been implemented so that incident closure has not been carried out optimally.

### 4.3 Problem management

Based on the results of interviews, questionnaires and data processing in this study, the results of data analysis are based on the stages of problem management which include 3 steps.

#### 4.3.1 Problem Identification

In ITIL a problem is defined as the cause or potential cause of one or more incidents. At this stage, the grouping of incidents into identified problems is carried out. can be seen in Table 8.

**Table 8. Problem Identification on LMS**

Incident or possibility incident	Problem Identification	IM ID
Earthquake	Natural Disasters	IM 1
Fire		
Abuse right access or user ID	Vulnerabilities and threats information	IM 2
Cybercrime		
Virus or malware attack		
Human error	Error from user	IM 3
Information data not accurate		
Failure system or unstable network	Maintenance system	IM 4
Failure or damage soft and hard device		
Disk Error or disk full		
Server Down		
Database Overload		
Technology Worn		
Due to server short circuit electricity		

Based on the results of problem identification, 4 problems were identified on the LMS, this is useful for the next stage which aims to analyze the identified problems and find the root causes and permanent solutions if possible.

#### 4.3.2 Problem control

At this stage, the problem is analyzed and the root causes are determined as well as finding permanent solutions or alternative solutions that can be used. as shown in Table 9.

**Table 9. Problem Control on LMS**

IM ID	Identificati on problem	Root of the problem	Possible solution applied
IM 1	Disaster natural	Disaster natural	This already applied to the LMS
IM 2	Vulnerabilities and threats information	There is gap from the LMS	Do prevention with periodic firewall updates, do 1 account for 1 access policy device.
IM 3	Error user	Negligence user in access or using an LMS	Do education in LMS use and doing fast response on every reported incident.
IM 4	Maintenanc e system	Monitoring is rare, there is no record of incidents or problems that have occurred.	Do periodic evaluation and monitoring with period more time often like 2 months once, start do recording incident.

Based on the results of problem control, the root cause of the problem can be found and a solution can be implemented.

### 4.3.3 Error Control

The fault control stage is carried out if a permanent solution cannot be applied due to various factors, then a temporary solution is needed that can be done to deal with the problem as soon as possible, as shown in Table 10.

**Table 10. Error Control on LMS**

IM ID	Identification problem	Temporary Solution
IM 1	Disaster natural	Permanent solution already applied to the LMS
IM 2	Vulnerabilities and threats information	Do restrictions Access and backup remaining data
IM 3	Error user	Handle events perceived by the user ,providing instructions for handling the incident experienced
IM 4	Maintenance system	Carry out monitoring at least 1 - 2 times one which year. This Already implemented by the LMS manager

### 4.4 SOP (Standard Operating Procedure)

SOP regulates the duties and functions of each element (implementer) in carrying out its role in the type of activity that involves more than one work unit / field of work. Therefore, the SOP is a document related to procedures or steps that will be carried out chronologically for a job in order to get maximum work results. SOP is needed to create a system that facilitates, tidies up, and brings order to a job and can be known by the person in charge of the activity if there is a deviation. There are several types of SOPs that are grouped in organizing activities such as SOPs based on the nature of activities, consisting of technical and administrative SOPs, SOPs based on the scope and magnitude of activities, consisting of macro SOPs and micro SOPs, SOPs based on the scope and completeness of activities consisting of final SOPs and partial SOPs, SOPs based on the scope and type of activities consisting of generic SOPs, namely SOPs that are compiled based on the nature and content of activities that are relatively similar both from activities that have standard operating procedures and from the stages of activities and their implementation. Variations in this SOP are based on differences in the location where the SOP is applied. Specific SOPs, namely SOPs based on the nature and content of activities that are relatively different from activities that have standard operating procedures such as stages of activities, actors (implementers) and where the SOP is applied. The format in the preparation of SOPs has several types including simple steps that contain few activities and require few decisions that are simple in nature, sequential stages which are formats for procedures that are compiled long exceeding 10 steps and require more detailed information but only require a little decision making, graphic formats are disusuh with long processes and are described into shorter sub-processes containing several steps, flowchart formats are used when making many decisions and require yes or no answer options.

SOP design will be made based on the solutions listed in Table 10 After the SOP has been designed, verification and validation will be carried out regarding the suitability of activities with the structure owned by e-learning management. Verification can result in changes to the design if needed to adjust the actual

situation and align with the ideal situation, while validation is done to prove the level of success if the SOP is implemented. The following is the draft SOP resulting from this research according to the results obtained from the analysis using event management and problem management with the type of Specific SOP with Hierarchical Steps format as shown in Table 11.

**Table 11. Standard Operating Procedure for handling incident and problem on LMS**

Activity	P.I.C	Form	Deadline
<b>Report incident or problem</b>			
Do verification to incident from user to service desk	Service desk	-	3 hours
Do recording on incident	Service desk	Record and report incident	2 hours
Do categorization incident.	Service desk	-	2 hours
Determine priority from incident	Service desk	Determination priority	2 hours
<b>Handling to incident</b>			
Coordination to BSI is responsible answer handle incident	Service desk	-	4 hours
Coordination to user	Service desk	-	3 hours
Confirmation from BSI incident handled	Service desk	-	2 hours
Make sure that problem has resolved	Service desk	Report about results	3 hours
Announce to user problem has resolved	Service desk	-	2 hours
Do closing events recorded incident	Service desk	Update Record incident	2 hours
<b>Evaluation</b>			
Inspect recording problems	Manager system (BSI)	-	2 months
Do trend analysis regarding frequent incidents	Manager system (BSI)	Report results analysis	2 months
Do monitoring to system at least 3 months in 1 time	Manager system (BSI)	Report monitoring results	3 months
Coordination to supplier (BSP or Server)	Manager system (BSI)	-	3 months

### 5. CONCLUSION

Based on the results of the analysis and discussion that has been carried out in this study, the conclusion is that in determining the level of ability based on ITIL, the results are obtained in

the form of incident management obtained the level of ability at level 2 and for problem management obtained the level of ability that is at level 1, through the stages of incident management and problem management practices in ITIL 4, a draft SOP (standard operating procedure) for handling the Ahmad Dahlan University LMS is obtained with 6 additional forms and 14 activities that can be carried out.

## 6. REFERENCES

- [1] R. Nurhidayat and S. Handayaningsih, "Risk Management Analysis of Student Resignation Services Using the COBIT 5 Framework Focus on Managing Risk (APO12)," *Journal of Informatics Engineering*, 2019.
- [2] A. Buana and A. Buana, "Measurement of Technology Acceptance Model (TAM) in Using E-Learning in Higher Education," *Journal of Information Technology and Education*, 2021.
- [3] A. Saepul, Y. C. Herry and A. Id Hadiana, "Information Technology Risk Management Based on the National Institute of Standards and Technology Sp800-30 at Universitas Jenderal Achmad Yani," 2017.
- [4] R. Ramadhan Putra, E. Setiawan and A. Ambarwati, "IT Risk Management Analysis on E-Learning Data Security and IT Assets Using NIST SP 800-30 Revision 1," *Journal of Informatics Engineering and Information Systems*, 2019.
- [5] A. Mukti Wibowo, *Introduction to IT Infrastructure Library Version 3*, 2018.
- [6] Musda, *An Introductory Overview of ITIL V3 A High Level Overview of the IT Infrastructure Library*, 2012.
- [7] anonim, "ITIL (Information Technology Infrastructure Library)," 2020.
- [8] Aisha Kusuma Wardani and L. Ramadani, "designing information technology service management governance using itil v3," 2016.
- [9] R. Witoko, "Analysis of Open-Ended Learning (OEL) Model with Assessment for Learning (AfL) in terms of Mathematics Learning Creativity," *Proceedings of the National Seminar on Mathematics*, 2019.
- [10] S. S. Putri, A. YS, S. Maftuhah and S. Sumiyati, "Assessment and Measurement of Teaching and Learning Outcomes from a Developmental Psychology Perspective," *anwarul*, 2023.
- [11] I. S. A. a. C. Association., *The risk IT framework : principles, process details, management guidelines, maturity models*, 2009.
- [12] P. Sarko and P. E. Rosalinda, "risk management Risk Identification and Measurement Methods RPS 2," 2019.
- [13] Kasidi, *Risk Management*, 2010.
- [14] G. B. Arumbinang and A. Tarigan, "internet service management governance concepts and strategies using the it infrastructure library for service-level agreements," *metik jurnal* , 2018.
- [15] A. Limited, *ITIL ® Foundation ITIL 4 Edition 2*, 2019.
- [16] A. K. Kaiser, *Become ITIL® 4 Foundation Certified in 7 Days*, 2021.
- [17] R. T. Hardika, "development of learning management system (lms) in the implementation of learning media in universities," *Prespektif*, 2021.
- [18] L. Hadisi and W. Muna, "information technology management in creating innovative learning models (e-learning)," *Journal Al-Ta'dib*, 2015.
- [19] B. S. M. Mustofa Pamungkas, *Guidelines for the Preparation of SOPs*, Jakarta: Lembaga Penjamin Mutu Unindra, 2021.
- [20] A. Abubakar, "Guidelines for the Preparation of Standard Operating Procedures for Government Administration," *Ministry of Administrative Reform and Bureaucratic Reform of the Republic of Indonesia*, Jakarta, 2012.
- [21] Listiawan, "development of learning management system (lms) in mathematics education study program stkip PGRI tulungagung," 2016.
- [22] I. B. G. Pujaastawa, "Interview and Observation Techniques for Information Gathering," 2016.
- [23] T. Meiriati, A. S. Sukanto and N. Mutiah, "ti asset management governance using cobit 5 and itam frameworks," *Journal of Computers and Applications*, 2020.
- [24] D. H. Satyareni and F. Mahanani, "Academic Information System Audit of XYZ College (PT) Using the COBIT 4.1 Framework," 2014.
- [25] Conner, *An Overview of the ITIL® Maturity Model*, 2021.