Risk Assessment Analysis using ITIL V.4 Framework on INLISLite

Suryahardi Ramadhan
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Integrated Library System (INLIS) Lite is an open-source web-based application designed to compile the national collection within the Indonesian National Digital Library network. It has been used by the Library Service Center of DPAD DIY to assist institutions in developing IT-based library processing and services. The aim of the risk assessment for INLISLite is not only to understand its management capabilities in dealing with various events and issues but also to prepare appropriate steps to handle problems or incidents that occur with INLISLite. This research was conducted by analyzing data obtained from observations using INLISLite, literature studies, interviews, and questionnaires. The collected data were then analyzed and mapped based on their levels. The capability level of INLISLite was determined using the ITIL V.4 framework. Based on this mapping and capability levels, an SOP (Standard Operating Procedure) design was created to address incidents and problems in INLISLite management. The results from the capability level assessment of INLISLite at the Library Service Center of DPAD DIY indicate that event management and problem management are both at level 2. This shows that the practices implemented in INLISLite are systematic and meet their objectives using a series of basic activities supported by specific resources. This research resulted in an SOP design based on ITIL 4 guidelines, with six additional forms out of fourteen activities.

Keywords

INLISLite, ITIL V.4, *Management Incident, Management Problem*, Draft SOP (*Standard Operating Procedure*).

1. INTRODUCTION

Information Technology (IT) in the era of the Industrial Revolution 4.0 is increasingly developing and changing the way humans solve problems in all types of work. Technological advancements have accelerated automation/computerization in business management. Computerization helps humans improve performance and save resources in the work process [1]. Information technology is a technology used to process data, including processing, obtaining, organizing, storing, and manipulating data in various ways to produce high-quality information that is relevant, accurate, and timely. This information is used for personal, business, and government purposes and is strategic for decision-making. The Integrated Library System (INLIS) Lite is an open-source web-based application developed by the National Library of Indonesia in 2011 to compile the national collection within the Indonesian National Digital Library network. It has been used by the Library Service Center of DPAD DIY to assist institutions in developing IT-based library processing and services [2]. The INLISLite system at the Library Service Center of DPAD DIY is used as a case study for this research, which is based on observations of INLISLite management. It was found that the INLISLite system still lacks adequate risk management, such as in the indexing of book data, which has become slow due to the large volume of data, and INLISLite has not yet structurally handled the risks, potentially causing the system to work suboptimally and face obstacles during use. Additionally, there is a need for a more specific SOP for managing incidents in the INLISLite system, as it can help manage incidents and issues to ensure the system operates optimally. Risk management is important to help administrators identify risks early, particularly in the context of problems that may arise from suboptimal system performance, which can disrupt INLISLite services. Through risk management, administrators can reduce potential threats and obstacles that may emerge, thereby ensuring the smooth use of INLISLite.

2. LITERATURE STUDY

2.1 Definition of Assessment

Assessment is a series of activities to systematically and continuously obtain, analyze, and interpret data about the learning processes and outcomes of students, making it meaningful information for decision-making [3]. The purpose of assessment is to answer questions, test hypotheses, or address specific problems using established scientific methods [4]. The goal of risk analysis is to separate small, acceptable risks from significant risks and to prepare data to aid in risk prioritization and management. Thus, in the context of analysis in risk management, it refers to a comprehensive understanding of the environment, objectives, resources, and parameters to be considered when identifying, assessing, managing, and monitoring risks within an organization or project. Context analysis is crucial to ensure that risks are correctly identified and managed in line with relevant objectives and environments.

2.2 Definition of Risk and Risk Management

risk is a condition that arises due to uncertainty, encompassing all unfavorable consequences that may occur [5]. Risk is the uncertainty that may result in a loss event [6]. Risk is the potential danger that may arise from certain current processes or future events [7]. Risk management is a strategy carried out to identify, manage, and evaluate all risks within an entity [8]. A risk is an adverse event or other definitions; the risk is the possibility of an outcome that does not match expectations. Risk arises due to uncertain conditions, risk is an event that occurs in a company that affects the achievement of the company's goals [9].

2.3 Risk Identification

Risk identification is a process that is systematically and continuously carried out to identify possible risks or losses to wealth, debt, and the company [10]. Risk identification is the effort to discover or recognize potential risks that may occur in the business processes of an organization or company. The purpose of risk identification is to identify all potential risks that may occur within an organization or company, typically caused by various factors, both internal and external [11].

2.4 Risk Management Process

Information technology risk management is an organization's ability to reduce IT risks that might hinder the achievement of organizational goals related to the use of IT itself [12]. The risk management process functions to make better decisions and improve efficiency. Risk management has three stages of the process, namely. Risk identification, evaluation, and risk assessment [13].The systematic application of policies, procedures, and management practices in the tasks of communicating, establishing context, identifying, analyzing, evaluating, handling, monitoring, and reviewing risks. Risk management becomes an essential element in the overall management process. Risk management involves many elements, and often, the best approach is to involve a multidisciplinary team. It is an ongoing process that involves iterative improvement steps. This process can be seen in Figure 1, which illustrates the risk management process.

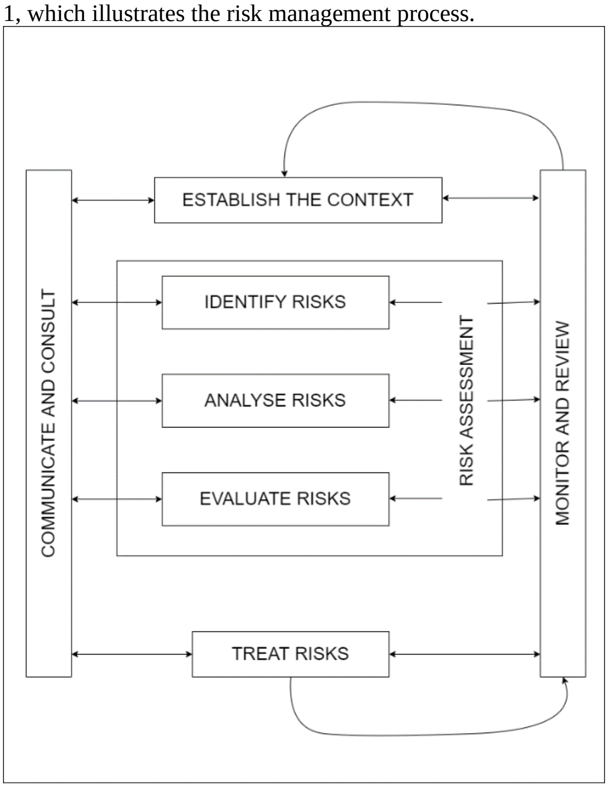

Figure: 1 Risk Management Process

This approach can be implemented in specific projects, aiding in specific decision-making or managing risks in particular areas. At each stage of the process, it is important to keep records to enable the understanding of decisions as part of the internal improvement process [14].

2.5 Types of Risk

Risks can generally be categorized into:

1. **Dynamic Risk**
   Dynamic risks often occur due to changes in economic situations, such as price levels, tastes, and rapidly developing technology. Management risks include various types of management risks, market risks, and risks resulting from innovation
2. **Static Risk**
   Static risks frequently occur in a static economic condition and do not change with the times. Static risks can be differentiated into pure risks and speculative risks.
   a. **Pure risk**
      Pure risk involves the possibility of an event occurring that is purely a risk, and the source of the risk is usually natural.
   b. **Speculative Risk**
      Speculative risk is the risk of profit and loss, as seen in gambling or trading. Speculative risk can result in either a chance of loss or a chance of gain, meaning the risk can lead to either a loss or a profit [15].

2.6 Analysis

In general, the definition of analysis is an activity consisting of a series of actions such as breaking down, differentiating, and sorting something to be re-grouped according to certain criteria, then looking for the relationships and interpreting the meanings. According to Komarudin (2001:53), the definition of analysis is a thinking activity to break down a whole into components so that the signs of the components, their relationships to each other, and their functions within an integrated whole can be recognized [16]. According to Prawiro (2020) [17], analysis is the effort to observe something in detail by breaking down its forming components or assembling those components for further study. Risk analysis is a process of evaluating the risks arising from existing hazards and providing adequate or appropriate controls over the existing controls. In the process of conducting a risk analysis, it is necessary to include various inputs of information and data as considerations to determine appropriate controls based on the level of existing risk [18].

2.7 Information Technology

The application of information technology has significantly advanced and played a crucial role, especially in the business world. According to Riskiono & Reginal (2018), information technology enables organizations to discover new business strategies, assists companies, organizations, schools, and governments in facing competition, and enhances productivity [19]. To optimize the use of information technology for business strategy purposes, its governance must be well-managed. Timely, secure, accurate, and relevant information technology services that meet user needs are crucial in supporting the smooth execution of library assessments. Maximum performance can be achieved if information technology's planning, strategy, and implementation are aligned. Technology is knowledge aimed at creating tools or actions for managing and creating objects. Meanwhile, information is something akin to data or something that will be conveyed from a source to an audience. Between technology and information, there lies an understanding where information technology encompasses everything related to the process of use as a tool, manipulation, and management of information. The integration of technology and information cannot be separated because it involves a very broad understanding related to the process, management, manipulation, and transfer of information across media [20].

2.8 INLISLite

INLISLite is a library automation software application developed by the National Library of the Republic of Indonesia (Perpusnas) in 2011. The name INLIS is derived from Integrated Library System, the name of the integrated library information management software built in 2003 for routine library information management activities within Perpusnas. INLISLite is an advanced development of the automation library software application INLISLite Version 3, built and developed by the National Library of Indonesia in 2011. INLISLite is developed as a one-stop software for library managers to implement library automation and manage digital collections, thereby serving as a digital library platform [21].

2.9 ITIL V4 Method

The ITIL framework has evolved over more than 20 years. As the most commonly used framework by many companies, its application in IT services proves that ITIL provides a practical reference framework, from planning identification to competent IT service support, thus encouraging many Service Management Layer (SML) practitioners in the industry to implement ITIL within their work scope [22]. ITIL stands for Information Technology Infrastructure Library. ITIL itself is an IT Service Management guideline. ITIL V4 is one of the latest versions of ITIL, with many updates, offering a more contextual and comprehensive ITSM (IT Service Management) practice by considering value streams and digital transformation, and incorporating new ways of working such as Agile, Lean, and DevOps [23]. ITIL presents a broad set of management procedures, which apply to all aspects of IT infrastructure, with which an organization can manage its IT operations [24]. ITIL V3 is a framework that was first released in 2007, underwent several updates in 2011, and most recently in 2017. It is the successor of the previous version (ITIL V2), which was first released in 2001. ITIL V3 brought changes to the IT service management framework from its predecessor by adopting a Service Lifecycle approach for integrating business and information technology solutions.

ITIL V4 brings updates by expanding the matured ITSM practices into a broader context, including user experience, value streams, and digital transformation. ITIL V4 provides the necessary guidance for organizations to face new challenges in service management and harness the potential of modern technology. ITIL V4 is designed to create a flexible, coordinated, and integrated system for effective service governance and management. In 2017, a new version of ITIL was announced, and two years later, in February 2019, the phased release of ITIL 4 began, with individual modules released over the following months. The core components of the ITIL V4 framework include the Service Value System (SVS) and the Four Dimensions Model. The ITIL SVS describes how various components and activities within an organization work together to create value through services that support information technology. The ITIL SVS facilitates integration and coordination while providing a strong, unified, and value-focused direction for the organization. The purpose of the Service Value System (SVS) is to ensure that the organization continuously creates value together with all stakeholders through the use and management of products and services within the ITIL SVS structure. The left side of the diagram shows opportunities and demands entering the SVS from both internal and external sources. The right side illustrates the value created for the organization, its customers, and other stakeholders. The structure of the ITIL SVS can be seen in Figure 2, which illustrates the service value system [25].

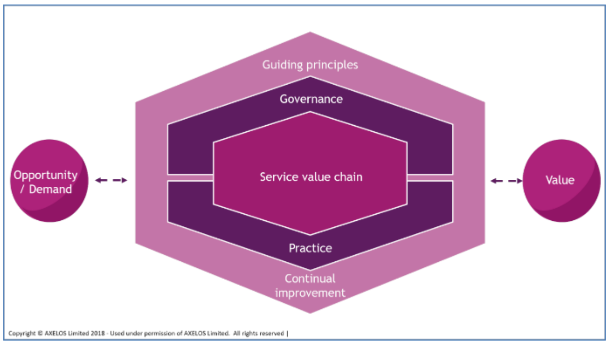

Figure 2: The Structure ITIL 4

To ensure a holistic approach to service management, ITIL 4 outlines the service management dimensions, where each component of SVS must consider these four dimensions: organization and people, information and technology, partners and suppliers, value stream, and processes. The central element of SVS is the service value chain, as depicted in Figure 3.

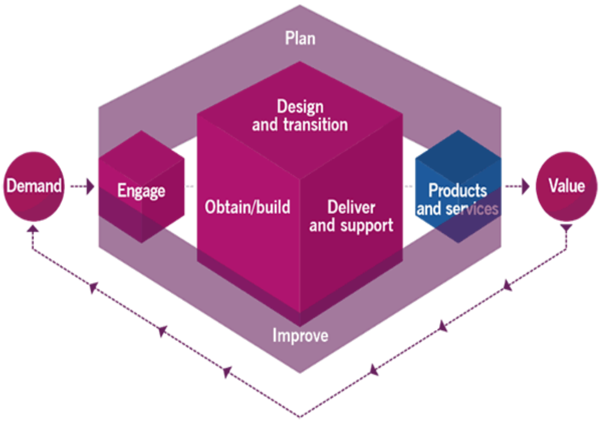

Figure 3: Service Value Chain

To ensure comprehensive adoption of the service management approach, ITIL V4 details the four service dimensions that should be considered in every component of SVS, as depicted in Figure 4.

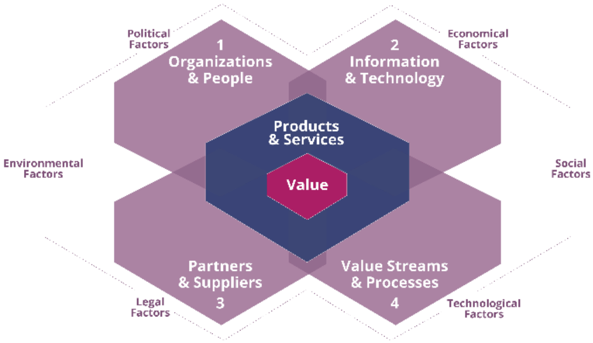

Figure 4: The Four Dimension

In this study, the practices used are incident management and problem management, where each domain has stages used to handle incidents and issues that occur [26]. Incident management consists of 7 stages, while problem management consists of 3 stages as shown in Figure 5 and Figure 6.

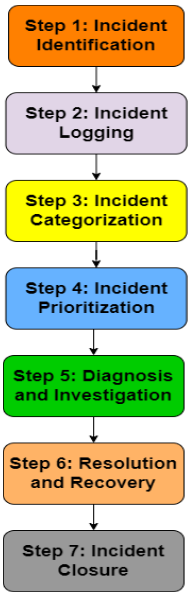
Step 1: Incident Identification
Step 2: Incident Logging
Step 3: Incident Categorization
Step 4: Incident Prioritization
Step 5: Diagnosis and Investigation
Step 6: Resolution and Recovery
Step 7: Incident Closure

Figure 5: Incident Management Steps

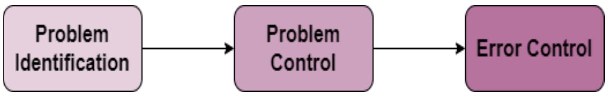

Figure 6: Problem Management Steps

3. METHODOLOGY

In this study, the method used is ITIL 4. The research involves several stages to gather the required data for analysis. These stages are as follows:

1. **Observation**
   Observation is the systematic observation and recording of phenomena visible in the research object. Observation is conducted at the DPAD DIY Library Service Center to directly observe the conditions in the field. This provides research material in the form of direct information from the DPAD DIY Library Service Center.
2. **Interviews**
   Interviews are a means of gathering relevant information for this research, specifically regarding the information technology risk management at the DPAD DIY Library Service Center. Interviews help in obtaining the necessary information and data for the research process. Interviews were conducted with Mr. Mohammad Hadi Pranoto, S.I.P., from the DPAD DIY Library Service Center.
3. **Questionnaire**
   A questionnaire was developed with several questions about incident management, incident handling duration, prioritization during incidents, incident recording, communication, and coordination related to incidents with the responsible team. Conversely, for problem management questions, it addresses recurring issues, how problem management functions to find short-term and long-term solutions, trend analysis, and collaboration to resolve complex problems. The RACI diagram was used to determine who would respond to this research questionnaire.
4. **Literature Study**
   In this literature study, reading and observing materials related to this research from reliable sources such as journals, the internet, and previous studies were conducted. The literature review serves as a way for the author to find supporting theories when analyzing information technology risk management, the subject of this research. These theories are relevant to risk management, ITIL V4, and similar studies to delve deeper into the research.
5. **RACI Diagram**
   RACI stands for Responsible, Accountable, Consulted, and Informed. RACI Chart functions at the level of the process of responsibility for roles in the organizational structure of the enterprise. COBIT 5 explains that the RACI Diagram is a matrix for all activities or decision authorities that must be taken within an organization associated with all parties or positions involved [27].

4. RESULT AND DISCUSSION

4.1 Capability Level

Based on the book "An Overview Of The ITIL Maturity Model" written by Adyrbai and published by Axelos in 2021, there are three assessment methods that can be used to determine the maturity level of ITIL. Each ITIL practice has capability levels measured by predefined capability criteria for each level. These criteria are designed to ensure comprehensive capability assessments that encompass the practice's ability to achieve its goals. To achieve this, the requirements should be based on Practice Success Factors (PSFs), which include components from the four dimensions of service management. Each PSF typically includes an average of 5-6 specified criteria. Fulfilling PSFs ensures the practice's objectives are met, and meeting PSFs is confirmed by satisfying all established criteria. Each criterion is mapped to one of the four service management dimensions and its respective capability level. The higher the capability level, the more comprehensive the expected realization of practices. Capability levels include scales that apply to each management practice, including:

1. Level 1: This practice is not yet well organized
2. Level 2: This practice systematically achieves its objectives through a series of basic activities supported by specific resources.
3. Level 3: This practice is well-defined and achieves its objectives in an organized manner, using specific resources and relying on inputs from other integrated practices within the service management system.
4. Level 4: This practice achieves its objectives in a highly organized manner, and its performance is continually measured and evaluated within the context of the service management system.
5. Level 5: This practice continually improves the organization's capability related to its objectives.

The overall capability level of ITIL practices is determined by the highest level where all capability criteria are met. Suppose all criteria mapped to Level 3 are fulfilled, and only some criteria mapped to Levels 4 and 5 are fulfilled. In that case, the overall capability level of the practice is assessed as Level 3 [28]. In this research, two PSFs were developed for incident management and one PSF for problem management. Capability levels were obtained from interview results and questionnaire analysis based on the compiled criteria. The results are then presented as shown in Table 1.

Table 1. Capability Level

Incident Management			
PSFs	**Capability Criteria**	**Dimension**	**Capability Level**
Ensuring that the process of identifying, addressing, and reducing the impact of incidents occurring on services is conducted optimally	The identification procedure has been adapted from relevant incident handling practices by INLISLite.	Value Stream and Process	2
	The procedure for establishing priority scales and categorizing incidents that have occurred or are identified to occur.	Value Stream and Process	3
Ensuring stable operational services of INLISLite that are responsive to occurring incidents	Efficient procedures for restoring services as quickly and effectively as possible	Values Stream and Processes	3
Problem Management			
PSFs	**Capability Criteria**	**Dimension**	**Capability Level**
Ensuring that prevention and problem handling are carried out optimally	Root cause analysis to prevent system disruptions.	Value Streams and Process	3
	Procedure for recording and documenting issues from incident reports.	Value Streams and Process	2
	Coordination of agreed-upon handling with the respective team.	Organization and People	4

So the results of the study indicate that in incident management, out of 2 PSFs with 14 criteria, it achieved level 2. This shows that the practices implemented in INLISLite are systematically carried out and meet their objectives through a series of basic activities supported by specific resources. Meanwhile, in problem management, out of 1 PSF with 6 criteria, it also achieved level 2. This indicates that the practices implemented in INLISLite are systematically carried out and meet their objectives through a series of basic activities supported by specific resources.

4.2 Incident Managament

Based on the results of interviews, questionnaires, and data analysis in this research, the data analysis results include seven steps in incident management. These steps are incident identification, incident logging, incident categorization, incident prioritization, diagnosis and investigation, resolution and recovery, and incident closure.

4.2.1 Incident Identification

The process of identifying past incidents in INLISLite will be conducted using brainstorming, based on interview results. The outcomes of this brainstorming session will be used to analyze and understand the issues that have occurred, allowing for the implementation of appropriate corrective measures to improve the quality and performance of INLISLite in the future. This is illustrated in Table 2.

Table 2. Incident Identification

Source Incident	ID	Incident or Possibility Incident
Natural	IK 1	Earthquake
	IK 2	Fire
Human	IK 3	Misuse of access rights or user ID
	IK 4	Human Error
	IK 5	Incorrect data information
	IK 6	Cybercrime
	IK 7	Data breach
System and Infrastructure	IK 8	Network system failure or network outage
	IK 9	Software failure or damage
	IK 10	Hardware failure or damage
	IK 11	*Disk Error* atau *disk full*
	IK 12	*Data Corrupt*

Based on the analysis, various potential incidents could impact INLISLite. These incidents are categorized into three main sources: natural, human, and system infrastructure. Of these three categories, two potential incidents from natural sources could cause damage to INLISLite. Five potential incidents originating from human sources could also have fatal consequences, and ten potential incidents from system and infrastructure sources could potentially disrupt INLISLite.

4.2.2 Incident Logging

In the incident logging stage, all identified incidents must be documented with the exact and immutable time of occurrence. This stage can be automated using various ITSM ticketing tools designed to record incidents. However, INLISLite has not yet implemented this automation, so the results displayed only show the frequency of incidents. This is evident in Table 3.

Table 3. Incident Logging

ID	Incident or Possibility Incident	Frequency Happened Incident
IK 1	Earthquake	≥ 1 times in 1 year
IK 2	Fire	≤ 1 times in 1 year
IK 3	Misuse of access rights or user ID	1-2 times in 1 year
IK 4	Human Error	2-4 times in 1 year
IK 5	Incorrect data information	1-2 times in 1 year
IK 6	Cybercrime	1-2 times in 1 year
IK 7	Data breach	1-2 times in 1 year
IK 8	Network system failure or network outage	1-2 times in 1 year
IK 9	Software failure or damage	1-2 times in 1 year
IK 10	Hardware failure or damage	≥ 1 times in 1 year
IK 11	Disk Error atau disk full	≥ 1 times in 1 year
IK 12	Data Corrupt	1-2 times in 1 year

Based on the recorded incidents, the most frequent issue is human error related to the use of INLISLite. This negligence can involve data input mistakes, such as entering inaccurate or incomplete information, selecting the wrong options or menus available in the system, and failing to follow established procedures. Additionally, human error can also occur due to insufficient understanding or inadequate training in using INLISLite, leading to users not fully mastering its functions and features. This often results in errors that can impact data quality and operational efficiency.

4.2.3 Incident Categorization

In the incident categorization stage, incidents or potential incidents will be grouped according to the need for appropriate handling and effective resolution. This categorization also facilitates the analysis of incident patterns, enabling the implementation of more targeted preventive measures. Consequently, each incident will be addressed based on its characteristics and urgency, ultimately improving the efficiency and effectiveness of the problem-solving process and minimizing the risk of similar incidents recurring. This can be seen in Table 4.

Table 4. Incident Categorization

ID	Incident or Possibility Incident	Category Handling
IK 1	Earthquake	Natural Mitigation Disaster
IK 2	Fire	Natural Mitigation Disaster
IK 3	Misuse of access rights or user ID	IT Personnel
IK 4	Human Error	IT Personnel
IK 5	Incorrect data information	IT Personnel
IK 6	Cybercrime	IT Personnel
IK 7	Data breach	IT Personnel
IK 8	Network system failure or network outage	The System Administrator
IK 9	Software failure or damage	The System Administrator
IK 10	Hardware failure or damage	The System Administrator
IK 11	Disk Error or disk full	The System Administrator
IK 12	Data Corrupt	The System Administrator

Natural disaster management, which specializes in handling emergencies to ensure safety and physical facility recovery. The IT team is responsible for system security issues, including data protection and cyberattack prevention, as well as addressing user-related issues. The system maintenance management team is responsible for infrastructure issues, including hardware maintenance, networks, and other operational environments. With this clear division of tasks, every aspect of potential issues can be effectively managed and responded to, ensuring the continuity of INLISLite operations and minimizing the impact of disruptions.

4.2.4 *Incident Prioritization*

In the incident prioritization stage, assessments are made to determine which incidents are most urgent, considering their urgency level and significant impact. This can be seen in Table 5.

Table 5. Incident Prioritization

ID	Incident or Possibility Incident	Incident Prioritization
IK 1	Earthquake	P1
IK 2	Fire	P1
IK 3	Misuse of access rights or user ID	P1
IK 4	Human Error	P1
IK 5	Incorrect data information	P2
Ik 6	Cybercrime	P1
IK 7	Data breach	P1
IK 8	Network system failure or network outage	P1
IK 9	Software failure or damage	P1
IK 10	Hardware failure or damage	P3
IK 11	Disk Error or disk full	P2
IK 12	Data Corrupt	P2

Based on interviews, the DPAD DIY Library Service Center team has set a maximum time limit of 2 days to resolve issues or incidents. Despite the priority system being implemented in INLISLite, its implementation is not yet optimal, leading to potential delays due to insufficient incident logging. The priority analysis results in three levels: P1 (urgent incidents to be resolved within 2 hours), P2 (moderate impact incidents to be resolved within 6 hours), and P3 (minor incidents to be resolved within 1 day).

4.2.5 *Diagnosis and Investigation*

The diagnosis and investigation stage is the initial step for IT personnel to understand and diagnose the root cause of user issues. This can be seen in Table 6.

Table 6. Diagnosis and Investigation

ID	Incident or Possibility Incident	Diagnosis and Investigation
IK 1	Earthquake	After the earthquake, INLISLite conducted a comprehensive inspection of its physical assets
IK 2	Fire	After the fire was extinguished, INLISLite conducted a thorough inspection of its physical assets
IK 3	Misuse of access rights or user ID	Checking users who have the same ID or show suspicious activity on their last access, such as data retrieval or modification, can be done to detect potential account abuse.
IK 4	Human Error	Ensure users understand and follow the appropriate steps to access the service or provide valid contact information when an error occurs due to user actions.
IK 5	Incorrect data information	Verify the data to ensure its accuracy and conformity with the information that should be
IK 6	Cybercrime	Examine INLISLite to identify and understand the cause of service disruptions.
IK 7	Data breach	Checking a user's recent accesses to identify potential suspicious activity, such as logins from unusual locations, accesses made at unusual times, or activity that does not match the user's profile.
IK 8	Network system failure or network outage	Inspect the network system and resolve any issues found
IK 9	Software failure or damage	Perform analysis to identify which parts of the software are failing or defective.
IK 10	Hardware failure or damage	Conduct checks to identify which parts of the hardware have failed or malfunctioned
IK 11	Disk Error or disk full	Perform disk checks to identify and correct errors, if still possible to access
IK 12	Data Corrupt	Investigate to identify the cause of inaccessible data

Based on the results of the diagnosis and investigation, a thorough examination of each incident is generally conducted to identify the root cause and find an effective resolution. This process involves in-depth analysis of the collected data and interviews with relevant parties.

4.2.6 *Resolution and Recovery*

Based on the results of the investigation, an appropriate resolution can be implemented to address the issue at hand. For events that are far-reaching and have the potential to affect many users, thorough testing should be conducted after the implementation of the solution to ensure that the issue is fully resolved and causes no further disruption. This can be seen in Table 7.

Table 7. Resolution and Recovery

ID	Incident or Possibility Incident	Resolution and Recovery
IK 1	Earthquake	Document damage to physical assets and identify interim solutions to address service failures resulting from such damage
IK 2	Fire	Reporting and finding temporary alternative solutions are important steps to ensure smooth service delivery.
IK 3	Misuse of access rights or user ID	Granting each user the minimum access rights necessary to perform their duties limits the potential damage if access rights are abused.
IK 4	Human Error	Identify factors that may increase the risk and assess past mistakes
IK 5	Incorrect data information	Rechecking the data to be changed to ensure its accuracy
IK 6	Cybercrime	Conduct simulations and training related to handling cybercrime to improve preparedness
IK 7	Data breach	Improve system security by identifying and preventing unauthorized or suspicious user activity
IK 8	Network system failure or network outage	Inform the responsible team regarding network problems in INLISLite to get solutions and improvements.
IK 9	Software failure or damage	Relay information related to software malfunctions to the IT team for follow-up.
IK 10	Hardware failure or damage	Ensure smooth operation of hardware by reporting problems to system maintenance and submitting appropriate repair or replacement requests.
IK 11	Disk Error or disk full	Inform system maintenance of detected disk errors or failures, and work with them to formulate effective long-term solutions for managing data storage.
IK 12	Data Corrupt	Report incidents of corrupt data to the IT team for in-depth investigation and analysis.

After finding solutions to problems that occur in INLISLite, IT personnel confirm to users and conduct regular monitoring after implementing the resolution. However, currently in the management of INLISLite, there is no reconfirmation regarding the handling of problems for users. Users only report the problems they face and then wait for resolution without any further confirmation.

4.2.7 Incident Closure

After the incident is resolved, confirmation is usually made with the user before closing the incident record. This confirmation is done by IT personnel to the user to ensure that the reported problem has been resolved properly. However, this process has not been running well in INLISLite, and there is no recording system implemented, so closing incidents has not been done optimally.

4.3 Problem Management

The results of data analysis in this study, which are based on the stages in problem management, consist of three main steps: problem identification, problem control, and error control

4.3.1 Problem Identification

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

Table 8. Problem Identification

Incident or Possibility Incident	Problem Identification	ID IM
Earthquake	Natural Disasters	IM 1
Fire		
Misuse of access rights or user ID	Information vulnerabilities and threats	IM 2
Human Error		
Incorrect data information		
Cybercrime		
Data breach	User error	IM 3
Network system failure or network outage		
Software failure or damage	System maintenance	IM 4
Hardware failure or damage		
Disk Error or disk full		
Data Corrupt		

Based on the identification results, four issues were found in INLISLite. This information is useful for the next stage, which aims to analyze these issues in detail, determine their root causes, and find permanent solutions if possible.

4.3.2 Problem Control

At this stage, a problem analysis is conducted to determine the root causes and to find permanent solutions or alternative solutions that can be implemented. This can be seen in Table 9.

Table 9. Problem Control

ID IM	Problem identification	root of the problem	Solutions that can be implemented
IM 1	Natural Disasters	Natural disasters	Establish procedures for dealing with natural disasters, this has been implemented in INLISLite.
IM 2	Information vulnerabilities and threats	Gaps in INLISLite	To prevent data corruption, regularly update the firewall and one account one device policies
IM 3	User error	User negligence in accessing or using INLISLite	To optimize the service process between IT personnel and users, learn how to use INLISLite, and respond quickly to any event reports.
IM 4	System maintenance	Monitoring is rarely conducted, and there is no incident recording and long-term planning with suboptimal priorities.	On a more frequent basis, such as every three months, conduct periodic evaluations and monitoring, start recording and documenting events or problems, and set priorities for addressing problems.

To optimize the INLISLite process, the results of issue control are used to conduct an in-depth analysis to identify the root causes of every issue that arises and to formulate appropriate solutions to ensure sustainability and optimal performance in data and information management.

4.3.3 Error Control

If a permanent solution cannot be implemented due to various factors, error control stages are carried out as an alternative measure. In this process, a temporary solution is needed to address the issue quickly and effectively, thereby minimizing any potential negative impact while waiting for the implementation of a more comprehensive permanent solution. As seen in Table 10.

Table 10. Error Control

ID IM	Problem Identification	Temporary Solution
IM 1	Natural Disasters	INLISLite already uses a permanent solution
IM 2	Information vulnerabilities and threats	Perform access restriction and save the remaining data
IM 3	User error	Handles events sensed by the user and provides instructions for handling the events
IM 4	System maintenance	Conduct monitoring at least one to two times each year, which has been done by INLISLite managers

The results of error control indicate that most processes are utilized in INLISLite and demonstrate effectiveness in managing data and information. In a more in-depth analysis, it was found that using INLISLite improves operational efficiency and helps maintain the accuracy and consistency of processed data. This proves that implementing INLISLite as an information management platform is very helpful in achieving broader organizational goals.

4.4 Standard Operating Procedure

SOP stands for 'Standard Operating Procedure'. It is a written document that regulates the steps or procedures to be followed in carrying out a specific task or activity consistently and efficiently. SOP is an important tool in operational management that helps ensure consistency, security, and effectiveness in carrying out daily tasks within an organization. Generally, SOPs regulate the tasks and functions of each element (executor) in carrying out their roles in activities involving more than one unit or field of work. Therefore, SOPs are documents related to procedures or steps that will be executed chronologically for a job to achieve optimal results. Standard Operating Procedures (SOP) are needed to create a system that simplifies, organizes, and regulates a job, as well as to identify the responsible party in case of any deviations [29]. Verification can result in changes to the design to adapt it to actual conditions and align it with the ideal state. Meanwhile, validation demonstrates that the Standard Operating Procedure (SOP) is successfully implemented. According to the analysis results, this is the SOP design generated from this study. Based on the analysis results, this is the SOP design generated from this research. This SOP uses incident management and problem management and is formatted with sequential steps (Hierarchical Steps) [30]. Hierarchical Steps is a development format of simple steps. This format is used when the procedure is lengthy, comprising more than ten steps, and requires detailed information but involves minimal decision-making. In hierarchical steps, the identified steps are elaborated into detailed sub-steps. As shown in Table 11.

Table 11. SOP for Handling Incidents and Problems on INLISLite

Activity	PIC	Form	Time Limit
Incident or Problem Report			
Following up on incident or issue reports from users to IT staff	IT Personnel	-	5 minutes
Compiling an official report on the incident or problem	IT Personnel	Recording and reporting incidents	5 minutes
Classifying incidents or problems based on their type, cause, or impact	IT Personnel	-	5 minutes
Prioritizing incidents or problems based on needs and resource availability	IT Personnel	Setting Priorities	5 minutes
Handling of Incident			
Contacting the authorized personnel at the DPAD DIY Library Service Office to resolve the issue	IT Personnel	-	5 minutes
Providing updated information to users about the progress of incident handling	IT Personnel	-	5 minutes
Receiving the official report from the DPAD DIY Library Service Center regarding incident resolution	IT Personnel	-	5 minutes
Ensuring that all root causes of the problem have been addressed	IT Personnel	The report on the test results conducted	10 minutes
Communicate to the users that the issue has been resolved and can be retried	IT Personnel	-	5 minutes
Record the final resolution of the incident	IT Personnel	Update of incident records	5 minutes
Evaluation			
Review event logs and issue report	The System Administrator	-	10 minutes
Analyzing incident data to find common root causes	The System Administrator	Analysis report	10 minutes
Conducting quarterly performance evaluations of the system	The System Administrator	Analysis report	10 minutes
Communicating incidents and issues to the service provider	The System Administrator		10 minutes

With 6 forms and 14 new activities identified to optimize the incident and problem management processes in INLISLite.

5. CONCLUSION

The results of determining the capability levels based on ITIL V4 guidelines with incident management and problem management processes in INLISLite indicate that both incident management and problem management are at level 2 concurrently. This means that the practices implemented in INLISLite are systematically achieving their goals through a series of basic activities supported by specialized resources. Based on the analysis in this study, a Standard Operating Procedure (SOP) design for handling incidents and problems in INLISLite at the Library Service Office of DPAD DIY has been developed using ITIL V4 practices, incorporating 6 additional forms and 14 activities. resolution and recovery tables are created in order to increase the capability level to the expected level. as seen in table 7.

6. REFERENCES

[1] Deyantoro, A. F., Setyadi, R., and Saintika, Y. (2022). The

Implementation of the Information Technology Infrastructure Library (ITIL) Version 3 Framework in the Service Operation Domain to Analyze Information Technology Service Management. JURIKOM (Journal of Computer Research), 9(3), 629–634.

[2] Moleong, G., and Tanaamah, A. R. (2022). Risk Analysis of Information Technology Using ISO 31000 on the Inlislite Application at the Archives and Library Office of East Nusa Tenggara Province. JATI (Journal of Informatics Engineering Students), 6(2), 501–506.

[3] Magdalena, I., Mulyani, F., Faridah, D. N., Fitriyani, N., dan Delvia, A. H. (2020). Analysis of the 2013 Curriculum Assessment System at SDN Bencongan 01. Journal of Education and Science, *2*(3), 333–341.

[4] Ghika Smarandana, Ade Momon, and Jauhari Arifin. (2021). Risk Assessment in the Manufacturing Process Using the Hazard Identification, Risk Assessment and Risk Control (HIRARC). Journal of INTECH Industrial Engineering Universitas Serang Raya, 7(1), 56–62.

[5] Wibawa, M. P., & Manuputty, A. D. (2020). Risk Management Analysis of Information Technology Policy Service PT. Asuransi Sinar Mas Using the COBIT 5 Framework. JATISI (Journal of Informatics Engineering and Information System), 7(3), 466–479.

[6] Thenu, P. P., Wijaya, A. F., & Rudianto, C. (2020). Analysis of Information Technology Risk Management Using COBIT 5 (Case Study: Pt Global Infotech). Journal of Bina Komputer, 2(1), 1–13.

[7] Pribadi, H. I., & Ernastuti, E. (2020). Information Technology Risk Management in the Implementation of E-Recruitment Based on ISO 31000: 2018 with FMEA (Case Study of PT Pertamina). Journal of Business Information System, 10(1), 28–35.

[8] Manuputty, G. P., Azis, A. A., and Pratami, N. A. N. (2019). Risk Management Analysis Based on ISO 31000 on the Operational Aspects of Information Technology PT Schlumberger Geophysics Nusantara.

[9] Dwianto, O., & Riadi, I. (2022). Risk Assessment Analysis of Medical Information System Services using COBIT 5 Framework. *International Journal of Computer Applications*, *184*(27), 7–17.

[10] Galeh, P., & Atmojo, M. B. T. (2021). Analysis of Information Technology Risk Management on UMKM Xyz Website Based on ISO 31000 Framework. Journal of Technology and Applied Business (JTTB), 4(1), 12–17.

[11] AS/NZS 4360:2004. (2004). Australian/New Zealand Standard Risk Management. *Australian Standards / New Zealand Standards 4360:2004*.

[12] Nuralim, E. B., and Riadi, I. (2021). Risk Assessment on Integrated Information Smart Service using COBIT 5 Framework. *International Journal of Computer Applications*, *183*(40), 14–21.

[13] Sukri, M., and Riadi, I. (2021). Risk Management Analysis on Administration System using OCTAVE Allegro Framework. *International Journal of Computer Applications*, *174*(17), 5–11.

[14] Arta, I. P. S., Satriawan, D. G., Bagiana, I. K., SP, Y. L., Shavab, F. A., Mala, C. M. F., Sayuti, A. M., Safitri, D. A., Berlianty, T., Julike, W., Wicaksono, G., Marietza, F., Kartawinata, B. R., & Utami, F. (2021). Risk Management, Theoretical and Practical Review. In Widina Bhakti Persada Publisher Bandung

[15] Rinaldi, A. D., and Riadi, I. (2023). Analysis of Learning Management System Service Risk Assessment using ITIL V4 Framework. *International Journal of Computer Applications*, *185*(36), 26–33.

[16] Septiani, Y., Aribbe, E., and Diansyah, R. (2020). Service Quality Analysis of Abdurrab University Academic Information System Toward User Satisfaction Using the Sevqual Method (Case Study: Abdurrab University Students Pekanbaru). Journal of Technology and Open Source, 3(1), 131–143.

[17] Faizal, M. I., Intan, V. N., and Firmansyah, R. (2021). Analysis of Management Information System for Education during the COVID-19. JEMSI (Journal of Economics, Management, and Accounting), 7(1), 9–16.

[18] Ernawati, and., & Prianjani, D. (2022). Risk Analysis of the Use of Personal Protective Equipment to Prevent COVID-19 Transmission. RADIAL : Journal of Science, Engineering, and Technology Civilization, 10(1), 120–131.

[19] Desy Ria, M., & Budiman, A. (2021). Design of Library Information Technology Governance Information System. Journal of Informatics and Software Engineering (JATIKA), 2(1), 122–133.

[20] Zahwa, F. A., dan Syafi'i, I. (2022). Selection of Information Technology-Based Learning Media Development. Equilibrium: Journal of Education and Economic Research, 19(01), 61–78.

[21] Zulhalim, Sulistyanto, A., and Sianipar, A. Z. (2019). Implementation of an Integrated Library Automation System Application Using INLISLite Version 3 at STMIK Jayakarta Library. JISAMAR (Journal of Information System, Applied, Management, Accounting and Research, 3(4*)*(4), 1–9.

[22] Prisetiahadi, M. A., Abdurrahman, L., dan Nugraha, R. A. (2021). Assessment of Information Technology Services Based on User Satisfaction Surveys with the Information Technology Information Infrastructure Library (ITIL) V3 Framework at PT. Transpotasi Jakarta (TRANSJAKARTA). 8(5), 9488–9496.

[23] Ada, S. T. R., Zahra, A. L., Shahita, D., Martapura, I. R., and Suryanto, T. L. M. (2022).Comparative Analysis of COBIT 5 and ITIL V4 in the Implementation of its Governance. Scan : Journal of Information and Communication Technology, 17(1), 23–29.

[24] R, R., Riadi, I., and Prayudi, Y. (2016). A Maturity Level Framework for Measurement of Information Security Performance. International Journal of Computer Applications, 141(8), 1–6.

[25] Kaiser, A. K. (2021). Become ITIL® 4 Foundation Certified in 7 Days: Understand and Prepare for the ITIL Foundation Exam with Real-life Examples. In Become ITIL® 4 Foundation Certified in 7 Days: Understand and Prepare for the ITIL Foundation Exam with Real-life Examples.

[26] Axelos. (2019). ITIL ® Foundation ITIL 4 EDITION.

[27] Waluyan, G., & Manuputty, A. D. (2016). Evaluation of

IT Governance Performance on the Implementation of Information System Starclick COBIT 5 Framework (Case Study: PT. Telekomunikasi Indonesia, Tbk Semarang). Nature, 249(5458), 668–670.

[28] Axelos. (2021). An Overview of the ITIL ® Maturity Model. Axelos.Com, September, 31.

[29] Syamsudin, A. (2012). Guidelines for the Preparation of Standard Operating Procedures for Government Administration. PERMENPAN Number 35 of 2012 concerning Guidelines for the Preparation of Standard Operating Procedures for Government Administration, 1-55.

[30] Mustofa, Pamungkas, B., & Salim, M. (2021). Guidelines for Developing Standard Operating Procedures (SOP) for Indraprasta PGRI University. 1–26.