Designing Risk Register And Risk Response As A Lesson Learned Towards The Ecohub Learning Management System Application Development Project at PT Xyz Using The Probability Impact Matrix Method

Dian Tri Athifah
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
dianathifah@telkomuniversity.ac.id

Dida Diah Damayanti
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
didadiah@telkomuniversity.ac.id

Sandhy Widyasthana
Faculty of Industrial Engineering
Telkom University
Bandung, Indonesia
sandhy@telkomuniversity.ac.id

Abstract*— The EcoHub Learning Management System (LMS) application development project at PT XYZ is a digital transformation initiative supporting organizational learning. As a software development project involving dynamic requirements and technological complexity, it is exposed to various risks disrupting objectives. Therefore, a structured qualitative risk management approach is required. This study applies the Probability Impact Matrix (PIM) method to conduct qualitative risk assessment and determine risk priority levels. A total of 30 potential risks were identified through expert interviews, project documentation review, and direct observation, covering technical, operational, human resource, security, organizational, and project management aspects. Each risk was assessed using the PIM framework and categorized according to severity. Risks with high priority were analyzed to develop suitable risk response management, including avoidance, mitigation, transfer, and acceptance. The main output is a comprehensive risk register integrating prioritized risks with corresponding risk response plans, serving as a lesson learned for the EcoHub project. The results provide a reference for future projects, highlighting how crucial early risk detection and organized risk response strategy are to improving project success.

Keywords—risk management, risk register, risk response, probability impact matrix, learning management system

I. BACKGROUND

The development of Learning Management Systems (LMS) has accelerated significantly with the increasing demand for digital learning systems, especially since COVID-19. This pandemic has been a major driver in accelerating digital transformation in the education sector and in business organizations. Learning Management Systems play an important role in supporting technology-based learning management by facilitating the distribution of materials, quizzes, interactions, and evaluations more effectively [1]. One of the parties contributing to supporting digital transformation in the field of education and training is PT XYZ, a consulting company engaged in strategy and business development, accounting and tax services, information technology development, training, education, and professional certification. In an effort to address these needs, EcoHub Learning Management System is presented as a digital learning solution based on Learning Management System (LMS) designed to improve the literacy and competence of Indonesia's workforce, particularly in the MSME sector and related training institutions.

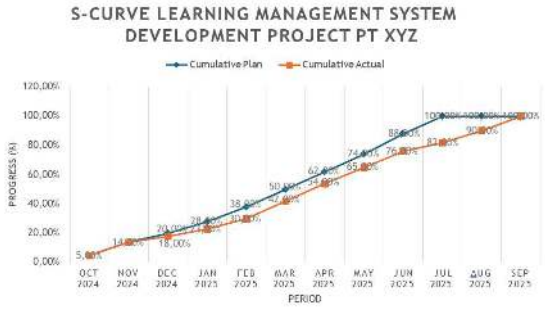


FIGURE 1
S-Curve EcoHub LMS System Project PT XYZ

The S-Curve functions as empirical documentation contrasting the planned cumulative progress with the actual realization of the EcoHub Learning Management System project at PT XYZ (October 2024–September 2025). The visualization demonstrates a pronounced performance deviation, most notably between December 2024 and May 2025, suggesting that critical risks regarding resource availability, stakeholder requirements, and technical complexity were not optimally identified. Despite the project ultimately achieving 100% completion in September 2025 through corrective measures, the execution phase encountered significant challenges and delays that necessitated project adjustments through addendums. These fluctuations indicate deficiencies in early-stage risk anticipation which contributed to deviations in time, cost, and scope. Therefore, this study reinforces the importance of systematically examining these historical shortcomings to develop a comprehensive Risk Register and Risk Response as a formal lesson learned for future system development projects.

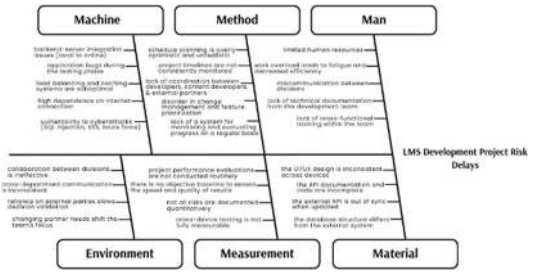


FIGURE 2
Project Risk Fishbone

Further analysis of the causes of project delays was conducted using a fishbone diagram that mapped the root causes into several main categories, namely people, methods, technology, environment, materials, and measurement. The results of the analysis show that issues such as limited human resources, changes in stakeholder requirements, inaccurate time estimates, and the technical complexity of the system were the dominant factors contributing to delays in the completion of project activities. These factors had a direct impact on reducing work efficiency, increasing the need for schedule adjustments and necessitating corrective actions during the execution phase. This condition emphasizes the importance of implementing structured and documented project risk management, particularly through the designing of a risk register and risk response as a lesson learned to prevent the recurrence of similar risks. According to the Project Management Institute and Kerzner, project risk management is a systematic process including risk management planning, identification, qualitative and quantitative analysis, response planning, implementation, and monitoring, where risk is defined as an uncertain event that may have either a positive or negative impact [2], [3]. From this viewpoint, risks are not merely treated as potential failures but also as strategic opportunities that can be managed to achieve optimal project performance; consequently, the use of analytical tools such as fishbone diagrams assists project teams in identifying the root causes of risks comprehensively.

One of the critical stages in this process is Perform Qualitative Risk Analysis, which utilizes the Probability Impact Matrix (PIM) to prioritize risks based on their probability of occurrence and the magnitude of their impact on project objectives. In addition to risk assessment, systematic risk identification plays a crucial role, where the implementation of a Work Breakdown Structure (WBS) supports the process by providing a hierarchical decomposition of the project scope into smaller, measurable activities. The integration of WBS and the Probability Impact Matrix enables the development of a more accurate risk map and supports the prioritization of risks that are relevant to actual project conditions. However, despite the completion of the EcoHub Learning Management System development project, PT XYZ does not yet possess a formally documented and structured risk register as a lesson learned. According to PMI (2017), the absence of a lesson-learned-based risk register increases the likelihood of similar risks recurring in subsequent system development projects. Therefore, this study focuses on designing a risk register and risk response plan as a formal lesson learned for the EcoHub Learning Management System development project at PT XYZ using the Probability Impact Matrix method, with results expected to serve as a reference for implementing more effective and structured risk management practices in future application development projects.

II. THEORETICAL REVIEW

A. Project Risk Management

According to Kerzner, the process of recognizing, evaluating, and addressing project hazards is known as risk management [2]. It entails minimizing the likelihood and effects of unfavorable events on project goals and optimizing the likelihood and effects of favorable events. The procedures of carrying out risk management planning, identification, analysis, response planning, response implementation, and risk monitoring on a project are all included in project risk management. Plan Risk Management, which is the process of determining how to carry out risk management activities for a project, is where the process starts. This process's main advantage is that it guarantees that the level, kind, and visibility of risk management are commensurate with hazards and the project's significance to the company and other stakeholders. Following this, Identify Risks is the process of identifying individual project risks as well as sources of overall project risk, and documenting their characteristics [2], [3].

B. Plan Risk Responses

Plan Risk Responses is the process of creating options, choosing tactics, and deciding on courses of action to manage both individual project risks and overall project risk exposure [3]. Strategies for risk response are categorized based on whether the risk is a threat (negative) or an opportunity (positive). Avoid, transfer, and mitigate are three tactics that usually address risks or hazards that could negatively affect project goals if they materialize. The fourth strategy, accept, can be used for negative risks or threats as well as positive risks or opportunities [3]. Avoid is a risk response strategy whereby the project team acts to eliminate the threat or protect the project from its impact. Transfer is a risk response strategy whereby the project team transfers both ownership of the response and the impact of a threat to a third party. Mitigate is a risk response plan in which the project team takes steps to lessen the likelihood or impact of a risk. Finally, Accept is a risk response plan in which the project team chooses to recognize the risk and wait to act until it materializes.

TABLE 1
Strategies for Negative Risks

Alternative Strategies for Threats	Description
Escalate	Escalate is appropriate when a threat is outside the project scope or beyond the project manager's authority. Such risks are managed at the program or portfolio level rather than at the project level. The project manager is responsible for notifying the appropriate stakeholders, and once escalated, these risks are no longer monitored by the project team, although they may be recorded in the risk register for reference.
Avoid	avoid is applied to high-priority threats either removing the danger or shielding the project from its effects. This strategy involves modifying the project plan, objectives, strategy, schedule, or scope to reduce the probability of occurrence to zero, including actions such as clarifying requirements, improving communication, or acquiring necessary expertise.
Transfer	transfer is a strategy that contains shifting the ownership and impact of a threat to a third party. This approach is typically implemented through contractual agreements such as insurance, performance bonds, warranties, or guarantees, often entails giving the party taking on the risk a risk premium.

Mitigate	mitigate is a strategy aimed at reducing the likelihood of a danger occurring and/or its effects. Mitigation actions are more effective when implemented early rather than after the risk has occurred. Examples include simplifying processes, increasing testing activities, selecting more reliable vendors, or developing prototypes to reduce uncertainty. When the probability cannot be reduced, mitigation efforts focus on minimizing the impact by addressing factors that influence the severity of the risk.
Accept	accept is a strategy in which the existence of a threat is acknowledged without taking proactive actions to address it. This approach is generally applied to low-priority risks or when mitigation is not feasible or cost- effective. Acceptance of risk can be either active or passive. Active acceptance involves preparing contingency reserves such as time, cost, or resources to

Three of the five strategies are specifically meant to deal with opportunities (positive risks). The fourth and fifth strategies, accept and escalate, can be used for negative risks or threats as well as positive risks or opportunities [3]. Escalate happens when the project team or the project sponsor concur that an opportunity is outside the project's scope or that the suggested reaction would go beyond the project manager's authority, a risk response strategy is suitable. For high-priority chances when the organization wishes to guarantee that the opportunity is fulfilled, exploit approach may be chosen. Transferring ownership of an opportunity to a third party so that it receives a portion of the reward should the opportunity materialize is known as sharing. An opportunity's likelihood and/or effect can be increased by using an enhance strategy.

TABLE 2
Strategies for Positive Risks

Alternative Strategies for Opportunities	Description
Escalate	escalate is applied when an opportunity surpasses the project manager's authority or is outside the project's scope. These opportunities are overseen at the organizational, program, or portfolio levels. Ownership is formally transferred after the project manager informs the appropriate party about the opportunity. The project team no longer keeps an eye on the opportunity after it has been escalated, however it might still be listed in the risk register for future reference.
Exploit	The exploit strategy is applied to high-priority opportunities to ensure that the opportunity is realized. This approach aims to capture the associated benefits by taking actions that increase the probability of occurrence to 100%.
Share	share is a tactic that involves transferring ownership of an opportunity to a third party so that, should the opportunity materialize, the advantages can be divided. In order to successfully actualize the opportunity for the project's benefit, this method necessitates choosing a suitable partner and may entail offering incentives or pay to the party taking advantage of the opportunity.
Enhance	The enhance strategy is utilized to boost an opportunity's likelihood and/or effect. Early enhancement moves are are typically more successful than attempts made after the chance arises. This strategy focuses on strengthening the causes of the opportunity to increase its likelihood or, when probability cannot be increased, on maximizing the potential benefits by targeting factors that influence the magnitude of the opportunity.
Accept	accept is a strategy in which the existence of an opportunity is acknowledged without taking proactive actions to pursue it. This approach is generally applied to low-priority opportunities or when exploiting the opportunity is not feasible or cost-effective. Acceptance can be active or

C. Probability Impact Matrix

Perform Qualitative Risk Analysis is the process of evaluating each project risk's likelihood of occurrence, impact, and other factors in order to prioritize it for more investigation or action. To facilitate this, the Probability and Impact Matrix is used. It is a grid that shows the likelihood of each risk occurring as well as how it would affect the project's goals if it did [3]. The chances and effects of the combinations specified in this matrix enable the division of individual project risk into priority groups. The risk management plan's definitions are used to evaluate the likelihood of occurrence and impact.

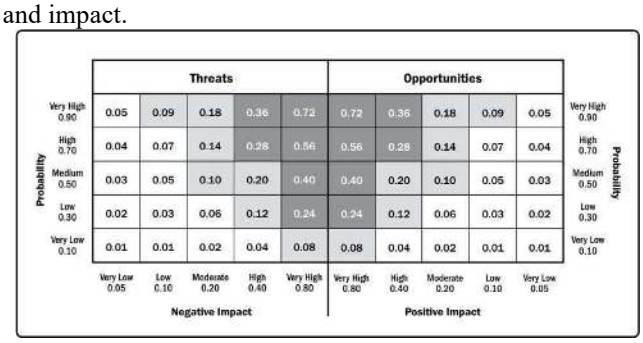


FIGURE 3
Probability Impact Matrix

III. METHODS



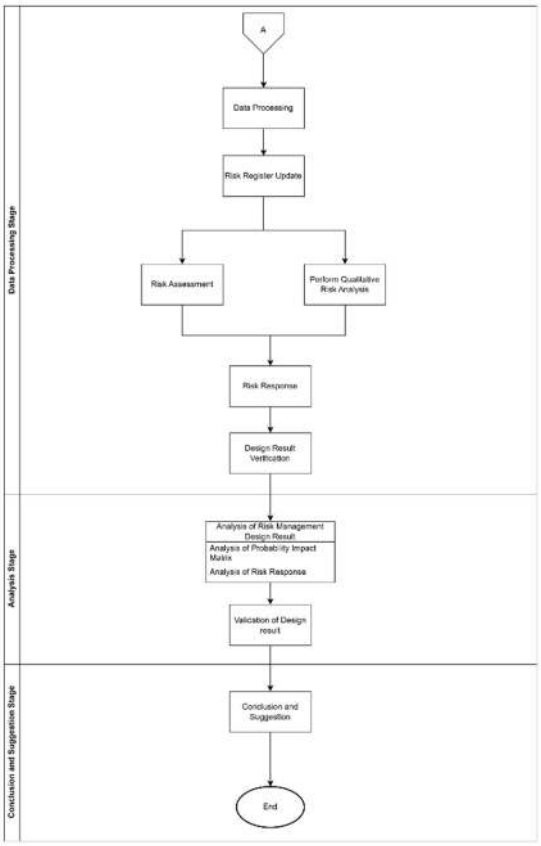


FIGURE 4
Systematic Design

Systematic design is a structured approach to be used in solving problems in this study. The stages of this systematic design consist of data collection, verification and validation of design results. The preliminary phase was conducted to gather information and identify the underlying issues involved in the development of the EcoHub Learning Management System application project at PT XYZ. The data collection stage is the process of searching for or gathering information necessary to achieve the research objectives, conducted through two sources: direct research (primary data) and available sources (secondary data). The data processing stage consists of a series of systematic steps to obtain previously collected data to produce a comprehensive risk management strategy, divided into three main interrelated stages: risk identification, risk assessment, and risk response. In the analysis stage, all identified and assessed risks will be comprehensively analyzed using the Probability Impact Matrix (PIM) approach to map the severity of risks that could hinder the success of the EcoHub Learning Management System application development project. This stage is the final stage of the research, where the author presents conclusions and suggestions based on the results of the research and risk analysis carried out related to the EcoHub Learning Management System (LMS) application development project at PT XYZ.

IV. RESULT AND DISCUSSION

Data collection in this study was conducted through project document studies, including the Statement of Work (SoW), Work Breakdown Structure (WBS), and Activity List, alongside interviews with parties directly involved to ensure risk identification was based on actual project conditions rather than theoretical assumptions [4]. The Statement of Work outlines the EcoHub Learning Management System application development project at PT XYZ, which aims to create a digital learning ecosystem to improve human resource competencies, particularly for MSMEs, with a scope covering system development, content development based on SKKNI standards, implementation and operations, and business development. The project follows a structured timeline from September 2024 to November 2025, divided into four phases ranging from research and concept formulation to the finalization of version 1.0, ensuring the system is technically stable and ready for large-scale implementation.

TABLE 3
Activity List

Activity ID	Activity Description	Estimated Duration (days)	Preceding Activities	Activity Owner
A1	Initial UI/UX design & module structure	30	-	Apps Development
A2	System architecture & database creation	21	A1	Apps Development
A3	Account registration system & dashboard development	39	A2	Apps Development
A4	Integration of basic features (videos, eBooks, quizzes, certificates)	43	A3	Apps Development
A5	Internal testing & debugging (Alpha Test)	7	A4	Apps Development
A6	Evaluation & reporting of system trial results	10	A5	Apps Development
A7	Integration of key features (certification, analytics, live sessions)	30	A6	Apps Development
A8	System performance & security optimization	22	A7	Apps Development
A9	Finalization of the LMS system	17	A8	Apps Development
B1	Curriculum design	10	-	Content Development
B2	Learning materials development	10	B1	Content Development
B3	Digital content production (eBooks, videos, slides, quizzes)	42	B2	Content Development
B4	Content review and editing	14	B3	Content Development
B5	Pilot class implementation and content testing	20	B4	Content Development
B6	Pilot result evaluation and content revision	14	B5	Content Development
C1	Digital training needs research & market analysis	14	-	Management
C2	Identification of competency gaps	15	C1	Management
C3	Development of a system blueprint & LMS business model	31	C2	Management

C4	Learning operations	20	C3	Management
C5	Evaluation of pilot results & product improvements	14	C4	Management
C6	Finalization of user guides & technical documentation	17	C5	Management
C7	Preparation for public launch & final stability testing	8	C6	Management
C8	BAST – Project Handover	6	C7	Management

A. Risk Register

Risk identification in this study was carried out by reducing the potential risks of each project activity listed in the WBS and Activity List. Each activity was analyzed to identify events that could potentially hinder the achievement of project objectives, in terms of time, cost, technical aspects, and safety. This WBS-based risk identification approach allows risks to be mapped systematically and specifically according to the application development stages. These results are in line with the findings of Sirait & Susanty (2016), which show that work process-based risk identification produces a more relevant and traceable list of risks compared to the general category-based approach [5]. Thus, the risks generated in this study reflect the actual conditions of the EcoHub Learning Management System application development project. All results of this process are presented in the risk register below.

TABLE 4
Risk Register

Risk Code	Activity Owner	Risk Type	Risk	Risk Description
R1.1	Apps Development	Threat	Backend and server integration issues	Obstacles in integration between the backend (local) and server (online) are one of the main causes of obstacles when the system is deployed to a production environment.
R1.2		Threat	Many bugs during testing	The discovery of several bugs in the LMS application during the testing phase also delayed the finalization process
R1.3		Threat	System instability after bug fixing	System instability due to code or configuration changes during the bug fixing and performance optimization process.
R1.4		Threat	Delay in bug fixing	Delays in bug fixes due to a queue of technical issues that need to be resolved gradually by a limited development team
R1.5		Threat	Changes in development priorities	Changes in development priorities, such as the emergence of requests for additional features or revisions from partners, which can shift the team's focus from maintenance activities to new development
R1.6		Threat	Lack of technical documentation	The lack of structured technical documentation means that code maintenance and error tracking take longer.
R1.7		Threat	Small changes cause system-wide issues	Minor modifications in one part of the system result in unexpected problems elsewhere.

R1.8		Threat	User data security risk	Sensitive user information could be exposed due to weak data protection mechanisms.
R1.9		Threat	Cyber-attacks (SQLi, XSS, brute force)	Vulnerability to cyber-attacks, such as Brute force login attempts, SQL injection, or cross-site scripting (XSS) that can disrupt the performance and integrity of systems
R1.10		Threat	Scalability issues	Where a significant increase in the number of users can reduce server performance if not balanced with adequate load balancing and caching systems
R1.11		Threat	Internet connection dependency	Dependence on an internet connection, which can affect the user experience in areas with unstable connections or low bandwidth
R1.12		Threat	Device compatibility	Differences in appearance and performance between devices (device compatibility), such as between desktops, tablets, and phones which can cause display inconsistencies, suboptimal navigation, or features that do not work perfectly on certain devices
R1.13		Threat	Limited server capacity during high traffic	A surge in the number of users causes a decrease in system performance and slower response times
R2.1	Management	Threat	Overly optimistic schedule planning	Overly optimistic schedule planning, especially in application development, has the potential to create a gap between plans and actual implementation in the field
R2.2		Threat	Lack of human resources	Limited human resources lead to duplication of duties, where one individual must take on responsibilities outside their primary job description. This increases the risk of work overload and reduces team efficiency

R2.3		Threat	Potential for miscommunication between divisions	Potential miscommunication between divisions in determining work priorities, resulting in some initial decisions not being fully integrated
R2.4		Opportunity	Flexible system blueprint	The initial planning evaluation helped the team build a flexible and reusable LMS system blueprint for future white-label projects
R2.5		Opportunity	Systematic planning structure	A systematic planning structure creates opportunities for the team to improve monitoring systems and increase transparency of progress across divisions
R2.6		Threat	Limited communication during remote collaboration	Remote working conditions reduce communication effectiveness and increase potential misunderstanding
R2.7		Threat	Lack of management supervision on maintenance progress	Weak oversight leads to unclear accountability and slower maintenance improvements.
R2.8		Opportunity	Business model opportunity “LMS as a Service”	This opened opportunities for the team to expand the business concept to "LMS as a Service," a model where the LMS system can be used by other partners with customized branding, content, and domains. This creates new commercialization potential because a single core system can be utilized by multiple institutions without the need for a complete rebuild
R2.9		Opportunity	External feedback improves UX	Feedback from external testers enhanced user experience, helping the system become more polished for future scaling
R3.1	Content Development	Threat	Delay in third-party content delivery	External content providers deliver materials late, slowing the completeness of learning content
R3.2		Threat	Misuse or piracy of digital content	Course materials or videos are used without official permission from the

				content provider
R3.3		Threat	Illegal content distribution (unauthorized link sharing or download bypass)	Users share direct download links or access premium content without authorization
R3.4		Threat	Double authentication issues (OAuth)	The difference in token standards and session management between the external system and LMS can cause login errors
R3.5		Threat	User data synchronization (duplicate accounts)	Differences in database structure can cause redundancy or account duplication
R3.6		Threat	External API dependency	If one of the systems updates without coordination, the integration can fail
R3.7		Threat	External system version incompatibility	When the LMS is upgraded, the old endpoint must remain compatible so that external systems are not disrupted
R3.8		Threat	Data loss risk due to backup or restore errors	User data security, including the possibility of personal information leaks due to vulnerabilities in authentication systems or data storage

B. Risk Assesment

Risk assessment were based on criteria to ensure consistency and reduce subjectivity in risk assessment. Risk assessment in this study is conducted qualitatively using an expert judgment approach to determine the probability of risk occurrence and the magnitude of its impact on the project. Probability and impact criteria were used as the basis for calculating risk scores and mapping risks using the Probability Impact Matrix (PIM) to group risks into watchlist and priority list categories. This approach is in line with Enterprise Risk Management practices that emphasize probability and impact-based risk assessment as the basis for determining priorities and risk response strategies [6]. The risk probability criteria in this study were compiled using a five-level scale representing the likelihood of risks occurring during the project implementation phase.

TABLE 4
Probability

Level	Score	Description
Very High	5	>70%
High	4	51-70%
Moderate	3	31-50%
Low	2	11-30%
Very Low	1	1-10%

TABLE 5
Criteria Negative Impact (Threats)

Aspect	Negative Risk Impact				
	Very low	Low	Moderate	High	Very high
	1	2	3	4	5
Time	Delay < 10%	Delay 10 – 20%	Delay 20 – 30%	Delay 30 – 40%	Delay > 40%
Costs	Cost increase <10%	Cost increase 10 – 20%	Cost increase 20 – 30%	Cost increase 30 – 40%	Cost increase >40%
Technical	Almost no effect	Decrease 10 – 20%	Decrease 20 – 40%	Decrease >40%	System Failure
Data Safety	No observable security	Minor security incident	Limited-impact breach	Major security	Critical system compromise

TABLE 6
Criteria Positive Impact (Opportunities)

Aspect	Positive Risk Impact				
	Very low	Low	Moderate	High	Very high
	1	2	3	4	5
Time	Time saving <10%	Time saving 10 – 20%	Time saving 20 – 30%	Time saving 30 – 40%	Time saving > 40%
Cost	Cost saving < 10%	Cost saving 10 – 20%	Cost saving 20 – 30%	Cost saving 30 – 40%	Cost saving >40%
	Negligible	Minor efficien	Moderate performa	Significant feature	State-of-the-art

Technical	improvement	cy increase	nce boost	improvement	system performance
Data Safety	Meets basic compliance	Enhanced local protection	Verified security resilience	Exceeds industry standards	Best-in-class security (Zero vulnerability)

Risk assessment is carried out using the Probability Impact Matrix (PIM) method by evaluating the probability and impact levels of each identified risk. The values are determined through expert judgement by the Project Manager of the EcoHub Learning Management System application development project at PT XYZ. The worst impact in terms of time, money, technical aspects, and safety is used to calculate the impact value. The risk value is then calculated by combining the likelihood and impact values, which is then mapped into the Probability Impact Matrix to determine the watchlist and priority list categories as the basis for preparing a risk response [4].

To illustrate the risk analysis mechanism within the EcoHub Learning Management System project, risks R1.2 and R2.4 were selected as calculation examples based on the PMBOK-aligned Probability Impact Matrix (PIM) framework. The total impact value for each risk was determined by identifying the maximum severity across time, cost, technical, and safety dimensions (Impact = MAX ($Impact_{time}$, $Impact_{cost}$, $Impact_{technical}$, $Impact_{safety}$), prioritizing the highest possible risk level rather than a cumulative sum. Applying this formula, risk R1.2 yielded a maximum impact of 5, while risk R2.4 resulted in an impact of 4. These values were subsequently multiplied by their respective probabilities (Risk Score = P x I) to derive the final risk scores, resulting in a score of 20 for R1.2 (4 x 5) and 12 for R2.4 (3 x 4).

TABLE 7
Risk Assesment

No	Risk Code	Risk Type	Risk	Probability	Impact-on				Risk Assessment	
					Time	Cost	Technical	Safety	Impact	Risk Score
1	R1.1	Threat	Backend and server integration issues	4	5	4	5	5	5	20
2	R1.2	Threat	Many bugs during testing	4	5	3	4	3	5	20
3	R1.3	Threat	System instability after bug fixing	4	3	4	4	3	4	16
4	R1.4	Threat	Delay in bug fixing	3	4	4	3	2	4	12
5	R1.5	Threat	Changes in development priorities	4	4	4	4	3	4	16
6	R1.6	Threat	Lack of technical documentation	4	5	4	4	4	5	20
7	R1.7	Threat	Small changes cause system-wide issues	2	3	3	3	3	3	6
8	R1.8	Threat	User data security risk	2	3	3	3	3	3	6
9	R1.9	Threat	Cyber-attacks (SQLi, XSS, brute force)	2	5	5	5	5	5	10
10	R1.10	Threat	Scalability issues	4	4	3	4	3	4	16
11	R1.11	Threat	Internet connection dependency	5	4	4	5	2	5	25
12	R1.12	Threat	Device compatibility	4	4	4	3	3	4	16
13	R1.13	Threat	Limited server capacity during high traffic	3	5	5	5	4	5	15
14	R2.1	Threat	Overly optimistic schedule planning	4	4	2	5	3	5	20
15	R2.2	Threat	Lack of human resources	4	5	3	4	3	5	20
16	R2.3	Threat	Potential for miscommunication between divisions	2	5	5	4	3	5	10
17	R2.4	Opportunity	Flexible system blueprint	3	4	2	4	4	4	12
18	R2.5	Opportunity	Systematic planning structure	4	5	5	5	4	5	20
19	R2.6	Threat	Limited communication during remote collaboration	4	4	3	4	3	4	16
20	R2.7	Threat	Lack of management supervision on maintenance progress	4	5	5	5	3	5	20
21	R2.8	Opportunity	Business model opportunity “LMS as a Service”	5	4	2	4	4	4	20

22	R2.9	Opportunity	External feedback improves UX	5	4	3	5	3	5
23	R3.1	Threat	Delay in third-party content delivery	3	4	3	4	3	4
24	R3.2	Threat	Misuse or piracy of digital content	4	5	3	4	5	5
25	R3.3	Threat	Illegal content distribution (unauthorized link sharing or download bypass)	5	5	3	5	5	5
26	R3.4	Threat	Double authentication issues (OAuth)	4	5	3	5	5	5
27	R3.5	Threat	User data synchronization (duplicate accounts)	4	5	4	4	3	5
28	R3.6	Threat	External API dependency	4	4	3	4	3	4
29	R3.7	Threat	External system version incompatibility	4	5	4	5	3	5
30	R3.8	Threat	Data loss risk due to backup or restore errors	4	3	3	3	3	3

C. Probability Impact Matrix

At this stage, based on the outcomes of the risk assessment procedure, each identified risk is given an effect value. The risk severity level is then determined by mapping each risk to a likelihood and impact matrix, which is then divided into high, medium, and low categories. The probability–impact matrix approach is widely used in previous research as a qualitative risk assessment tool to determine risk management priorities [7].

TABLE 8
Probability Impact Matrix

Threat						Opportunity					
Probability	5					R1.11, R3.3	R2.9	R2.8			5
	4			R3.8	R1.3, R1.5, R1.10, R1.12, R2.6, R3.6	R1.1, R1.2, R1.6, R2.1, R2.2, R2.7, R3.2, R3.4, R3.5, R3.7	R2.5				4
	3					R1.4, R3.1	R1.13		R2.4		3
	2				R1.7, R1.8		R1.9, R2.3				2
	1										1
		1	2	3	4	5	5	4	3	2	1
		Impact					Impact				Probability

All identified risks were assessed using the expert judgement method by the project manager, considering the probability values and the impacts of the risks on time, cost, technical and safety aspects. The assessment results were then used to calculate the risk scores and to map each risk into the Probability Impact Matrix. Based on the Probability Impact Matrix mapping results, the project was identified to have 22 risks with high severity, 8 risks with medium severity, and no risks with low severity, resulting in a total of 30 identified risks. Risks categorized as high and medium severity were further classified as priority risks requiring special attention in the risk management process, while low-severity risks were included in the watchlist category.

D. Risk Register Update

The following Risk Register Update table shows the results of the risk register update after assessing the probability and impact values on several aspects, namely time, cost, technical, and safety. Furthermore, impact and Expected Value (EV) calculations were performed at the risk assessment stage. This risk register update is the final documentation of the design results developed in this study. The design results are expected to be used and implemented by the Project Manager of the EcoHub Learning Management System application development project at PT XYZ as a reference in project risk management [7].

TABLE 9
Risk Register Update

Risk Code	Risk Type	Risk	Probability	Impact	Risk Score	Severity Level	Risk Responsibility
R1.1	Threat	Backend and server integration issues	4	5	20	High	System Analyst
R1.2	Threat	Many bugs during testing	4	5	20	High	System Analyst
R1.3	Threat	System instability after bug fixing	4	4	16	High	System Analyst
R1.4	Threat	Delay in bug fixing	3	4	12	Medium	Project Manager
R1.5	Threat	Changes in development priorities	4	4	16	High	Project Manager

E. Risk Response

Each risk has been identified and analyzed, and then ddressed by establishing the most relevant response strategy. The strategic approaches applied include escalate, accept, avoid, mitigate, and transfer for negative risk categories, and exploit, enhance, share, accept, and escalate for positive risks. The selection of these response types is based on considerations of urgency, significance of impact on project objectives, and efficiency of available resources. To ensure effective handling, each strategy implemented requires consistent monitoring and periodic evaluation so that it can be adjusted to the dynamics of project changes [7].

TABLE 10
Risk Response

Risk Code	Risk	Risk Severity	Risk Response
R1.1	Backend and server integration issues	High	Mitigate
R1.2	Many bugs during testing	High	Mitigate
R1.3	System instability after bug fixing	High	Mitigate
R1.4	Delay in bug fixing	Medium	Accept
R1.5	Changes in development priorities	High	Mitigate

Mitigate is the most dominant strategy used, accounting for 60% of the total risks. This strategy focuses on actions to reduce the probability or impact of risks to an acceptable level. This is in line with the principle of risk management to proactively reduce the impact of risks before they occur [2]. The Avoid strategy is used for 10% of risks, primarily for high-impact risks that can be eliminated by changing plans or processes. The Transfer strategy accounts for 7% of risks, involving the transfer of risk responsibility to third parties, such as vendors or partners. Meanwhile, the Exploit and Enhance strategies are used for positive risks (opportunities), each accounting for 7% and 3% respectively, to maximize the benefits of the opportunities that arise. Finally, the Accept strategy is not used in this response plan, indicating that all identified risks are considered significant enough to require active handling rather than just being accepted passively.

F. Verification and Validation of Design Results

The design results verified include risk register updates, risk responses, and risk register templates, aiming to ensure that all design results are in line with the research objectives and can be effectively applied in risk management. The content in risk register updates includes risk probability values, risk impact amounts, risk score calculation results, risk response strategies, and other relevant information that supports risk management [3]. Furthermore, validation was carried out on the risk register update design through interviews with the Project Manager on the EcoHub Learning Management System application development project at PT XYZ. The results of the validation process confirm that risk register updates are designed in accordance with PMBOK risk management standards, including a complete list of risks, risk owners, probability values, impacts, and risk scores. Additionally, the risk response strategies, mitigate, avoid, transfer, and accept, are in line with the severity level of the risk, and the template is confirmed to be compliant with project risk management requirements, easy to use for non-technical users, accessible via Google Sheets, and supportive of regular risk monitoring and updates.

V. CONCLUSION

This study successfully identified 30 project risks, consisting of 24 negative risks (threats) and 6 positive risks (opportunities). The risk identification process was carried out systematically through a review of project documents, namely the Work Breakdown Structure (WBS), Statement of Work (SoW), and Activity List, reinforced by expert judgment. Risk assessment was conducted using the Probability Impact Matrix (PIM) method, showing that all identified risks fell into the priority risk category with medium and high severity levels, such as changes in user requirements and developer resource constraints. Consequently, risk management strategies were developed referencing standards proposed by the Project Management Institute (PMI), utilizing mitigate, accept, transfer, and enhance strategies summarized in a risk register to serve as a lesson learned for future application development projects.

Based on these conclusions, it is recommended that the results of the risk analysis be actively utilized as a reference in every stage of planning, implementation, and evaluation, rather than just serving as documentation. PT XYZ is advised to form an internal risk management team to periodically review the risk register and to improve the competence of human resources through structured technical training programs and the formulation of Standard Operating Procedures (SOPs). Furthermore, for future researchers, it is recommended to develop this research by using more comprehensive quantitative approaches, such as Cost-Risk Analysis, Failure Mode and Effect Analysis (FMEA), or Monte Carlo Simulation, and to expand the scope of analysis to the post-implementation stage, including operational and user adoption risks, to provide more in-depth contributions.

REFERENCES

[1] H. Elmunsyah, A. Nafalski, A. P. Wibawa, and F. A. Dwiyanto, “Understanding the Impact of a Learning Management System Using a Novel Modified DeLone and McLean Model,” *Educ. Sci. (Basel).*, vol. 13, no. 3, p. 235, Feb. 2023, doi: 10.3390/educsci13030235.

[2] Harold. Kerzner, *Project management : a systems approach to planning, scheduling, and controlling*. John Wiley & Sons, Inc., 2022.

[3] Project Management Institute, *A guide to the project management body of knowledge*. Project Management Institute, Inc., 2017.

[4] A. Nehari Talet, “RISK MANAGEMENT AND INFORMATION TECHNOLOGY PROJECTS,” *International Journal of Digital Information and Wireless Communications*, vol. 4, no. 1, pp. 1–9, 2014, doi: 10.17781/P001078.

[5] N. M. Sirait and A. Susanty, “ANALISIS RISIKO OPERASIONAL BERDASARKAN PENDEKATAN ENTERPRISE RISK MANAGEMENT (ERM) PADA PERUSAHAAN PEMBUATAN KARDUS DI CV MITRA DUNIA PALLETINDO,” *Industrial Engineering Online Journal*, vol. 5, no. 4, 2016.

[6] K. Al-Amri and Y. Davydov, “Testing the effectiveness of ERM: Evidence from operational

losses," *J. Econ. Bus.*, vol. 87, pp. 70–82, Sep. 2016, doi: 10.1016/j.jeconbus.2016.07.002.

[7] S. Sufa'atin, "Implementasi Probability Impact Matriks (PIM) Untuk Mengidentifikasi Kemungkinan dan Dampak Risiko Proyek," *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, vol. 8, no. 1, pp. 43–47, Jun. 2017, doi: 10.31937/si.v8i1.555.