Condo Management System

RISK ASSESSMENT AND MANAGEMENT PLAN

Version *2.0*

03/03/2024

1 INTRODUCTION

1.1 PURPOSE OF RISK ASSESSMENT AND MANAGEMENT PLAN

A risk is a potential problem that can occur. It can have harmful consequences on the project's objectives in the future. Risk management is to identify and evaluate potential problems before they occur. The objective is to develop a plan to effectively address and mitigate risks.

The Risk Assessment and Management Plan (RMP) is an important document. It provides the team important information on possible problems. This helps the team to make informed decisions and prioritize tasks and risks during the project. The RMP will be monitored, documented and updated throughout the entire project lifecycle.

2 RISK MANAGEMENT PROCEDURE

2.1 PROCESS

All team members working on the project will be identifying, analyzing and managing risks throughout the project lifecycle. To reduce project delays and impacts, risks will be identified and accessed in the early stages of the project. To ensure that the documentation follows the RMP guidelines, one team member will be the Risk Manager (Vanisha Patel).

2.2 RISK IDENTIFICATION

To identify, document and manage risks during the project's lifecycle, there are going to be weekly team meetings to discuss and review each team member's progress on their assigned tasks to encourage team members to share any issues or challenges that they face because they could become risks. A risk analysis log file is accessible to all team members. The risk manager will take note of the concerns and analyze the risk identified.

2.3 RISK ANALYSIS

The team is using qualification analysis and is reporting the level of risk in the Risk Reporting Matrix to prioritize what risks should be addressed and which can be ignored. All risks identified are analyzed in a risk analysis table that provides information on ranking, threats, vulnerabilities, contextual factors, risks, likelihood, impact, reduction of threats, reduction of vulnerabilities and level of residual risk. These fields are analyzed by the risk manager.

2.4 RISK RESPONSE PLANNING

In the Risk Reporting Matrix, the risks will either be in the green, yellow or red zone. The risks can be addressed by avoiding, mitigating, accepting or transferring. Team members will be assigned to monitor risks falling in the red and yellow zone.

- **Avoid:** Avoiding the risk by avoiding the cause of this risk.
- **Mitigate:** Mitigating risk by minimizing its impacts on the system.
- **Accept:** Accepting the risk - nothing to be done.

To mitigate risks, the team members will find solutions to prevent risk from happening and reduce its impact and probability. The solution will be proposed to the Risk Manager and the manager will be verifying the solution's feasibility and will add and assign additional risk prevention tasks in the project schedule. This will minimize risk impacts.

2.5 RISK MONITORING, CONTROLLING, AND REPORTING

Important risks will be assigned to team members for monitoring, controlling and reporting during the project. The risk manager will be notified of project changes resulting from risk monitoring and controlling. Risks will be reported in the risk analysis table.

3 TOOLS AND PRACTICES

The risk analysis table serves as a log for risks for all team members. It will be maintained by the risk manager to ensure that it follows formatting guidelines. The Risk Reporting Matrix will be used for qualification analysis.

4 RISK ANALYSIS AND MANAGEMENT

4.1 RISK ANALYSIS TABLE

The risk analysis table helps to understand the severity of the risk by ranking them. The required information in the table are ranking, threats, vulnerabilities, contextual factors, risks, likelihood, impact, reduction of threats, reduction of vulnerabilities and level of residual risk. It helps the team to decide on how to address the risk.

The detailed risk analysis table can be found in the file Risk Analysis.xlsx. Examples of two risks related to the condo management system project are shown in Figure 1.

Risk ID	Ranking	Threats (1)	Vulnerabilities (2)	Contextual factors	Risks (3)	Likelihood from 1 to 5	Impact from 1 to 5	Reduction of Threats (Acceptance Strategy)	Reduction of Vulnerabilities (Protection Strategy)	Level of residual Risk
1	9 - Medium	Unauthorized access to User's Profile	- User has a weak password - Sign up does not enforce complex password format - The passwords stored in the database are not encrypted - No multi-factor authentication	- Cyber attacks are common in in software that handles properties and finances - User's use unsecured public network	To be subjected to unauthorized access to user's sensitive data	2	5	- Monitor unusual user activities - Warn users of potential cyber attacks when creating an account	- Implement strong password requirement when user signs up - Implemented strong encryption for passwords - Implement multi-factor authentication	6 - Low
2	16 - High	Insufficient system testing	- The test coverage is low which causes undetected bugs and system failures - Inadequate compatibility testing - Incomplete exeption and error handling - Incomplete security testing	- Insufficient testing caused by tight sprint deadlines - Testing inefficient because of frequent changes in the code	To be subjected to software crashes and security vulnerabilities	5	4	- Allow users to report bugs on the application/website - Train the entire team on software testing and bug reporting	- Write unit, integration and system tests - Reserve five days before deadline for system testing and fixing bugs and error handling - Attain a test coverage of 80%	8 - Medium

Figure 1: Examples of risks from Risk Analysis.xlsx file

4.2 RISK REPORTING MATRIX

The risks identified in the risk analysis table are presented in the risk reporting matrix to visualize its severity. The list of identified risks shown in table 1 is a summary of the content of the risk analysis file. The risk reporting matrix is shown in figure 2. The risks are represented by their risk ID.

The risk manager analyzes the probability and impact of each identified risk.

Risks Probability:

- **High:** Greater than 70% probability of occurrence
- **Medium:** Between 30% and 70% probability of occurrence
- **Low:** Below 30% probability of occurrence

Risk Impact:

- **High:** Risk that has the potential to greatly impact project cost, project schedule or performance
- **Medium:** Risk that has the potential to slightly impact project cost, project schedule or performance
- **Low:** Risk that has relatively little impact on cost, schedule or performance

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
R-1	**Security:** Unauthorized access to user's profile	Medium	TBD	Mitigate
R-2	**Technical:** Insufficient system testing	High	2	Mitigate
R-3	**Security:** Data Breach	Medium	TBD	Accept
R-4	**Management:** Poor communication within team	Medium	2	Mitigate
R-5	**Management:** Unqualified teammates for mobile app development	High	TBD	Accept
R-6	**Requirements:** Poor requirements definition	Medium	TBD	Mitigate
R-7	**Data:** Condo owner dashboard displaying incomplete or inaccurate information	Low	TBD	Mitigare
R-8	**Security:** User forgets password and is not able to access their account	High	TBD	Mitigate
R-9	**Data:** Managing large numbers of documents	Low	2	Accept
R-10	**Data:**	Low	TBD	Accept

	Data access violation for condo management companies information			

Table 1: List of identified risks

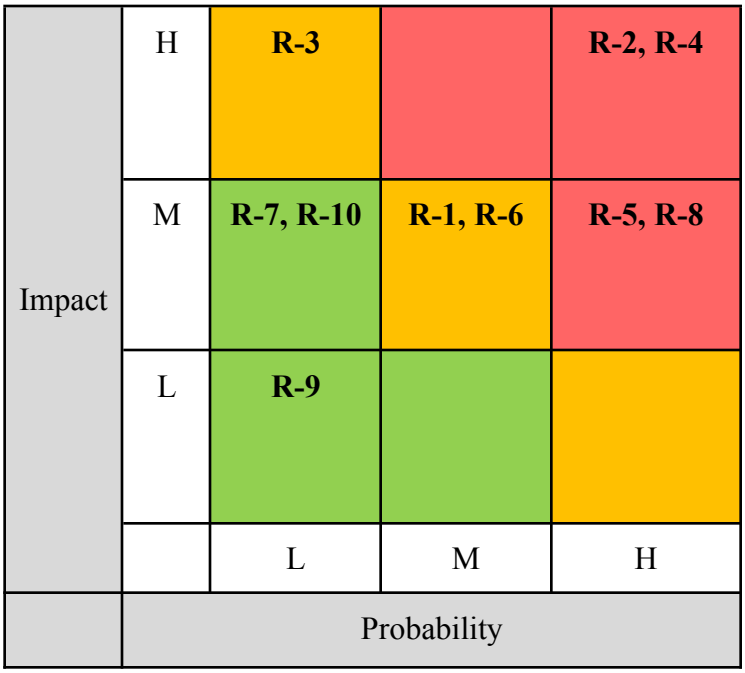

Figure 2: Risk Reporting Matrix