ROOMIELAH

RISK MANAGEMENT PLAN

Version 1.1
03/15/2022

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Atul Acharya	03/01/2022	Srishti Arora	03/05/2022	Initial Risk Management Plan draft
1.1	Aks Tayal	03/14/2022	Srishti Arora	03/15/2022	Update Risk Management Plan

UP Template Version: 11/30/06

TABLE OF CONTENTS

1 INTRODUCTION **1**
1.1 Purpose Of The Risk Management Plan 1
2 RISK MANAGEMENT PROCEDURE **1**
2.1 Process 1
2.2 Risk Identification 1
2.3 Risk Analysis 1
2.3.1 Qualitative Risk Analysis 1
2.3.2 Quantitative Risk Analysis 2
2.4 Risk Response Planning 2
2.5 Risk Monitoring, Controlling, And Reporting 2
3 TOOLS AND PRACTICES **2**
RISK MANAGEMENT PLAN APPROVAL **3**
APPENDIX A: REFERENCES **4**
APPENDIX B: KEY TERMS **5**

1 INTRODUCTION

1.1 PURPOSE OF THE RISK MANAGEMENT PLAN

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the RoomieLah project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.

The Risk Management Plan is created by the project manager in the Planning Phase of the CDC Unified Process and is monitored and updated throughout the project.

The intended audience of this document is the project team, project sponsor and management.

2 RISK MANAGEMENT PROCEDURE

2.1 PROCESS

The Project Manager will serve as the Risk Manager for this project. The project manager, working with the project team and project sponsors, will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections:

2.1.1 Risk Identification

The team will identify potential risks that may affect the project. During the process, they will also need to consult others or conduct discussions for areas outside their expertise like compliance, legal, regulatory, and market risks. The team will also refer to documentation of past projects undertaken by different teams to draft a skeleton and use scenario analysis to check if the risk is applicable to our project. The risks identified during the discussions are documented for further analysis.

2.1.2 Risk Analysis

After documenting all the potential risks, the team will collectively perform quantitative and qualitative analysis. The intention is to estimate the scope of the risk and identify the range of possible outcomes. The standalone risks will be assessed individually; risk models or risk trees (trees that visualize the chronological events needed for the risk to actualize) will be created to estimate the likelihood of the risk occurring. The collated analysis will enable the team to make decisions based on the knowledge from the results.

2.1.3 Risk Response Planning

The next step is to decide on plans to minimize the effect of risks based on information collated from the previous step. Brainstorming is required to draw up a plan of action to avoid or mitigate certain risks. The team will also draw up contingency plans for risks that are inherent to the project i.e. cannot be avoided or mitigated.

2.1.4 Risk Monitoring and Control

Certain categories of risks (based on the scope and likelihood) will be closely monitored by the team members. The team members will ensure that an avoided or mitigated risk is not realized. The team will also need to take appropriate action to control the impact of unforeseen risks or inherent risks when realized.

2.2 RISK IDENTIFICATION

Risk Identification is the process through which, risks which could potentially prevent the program, enterprise or investment from achieving its objectives. This is the most crucial step as the risk needs to be identified first before it can be reduced, mitigated or transferred.

A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located at the project's SVN and Wiki.

Risks identified are broadly classified into six categories - Technology, People, Organizational, Tools, Requirements and Estimation.

	Risk Category	Risk Examples
1.	Technology	1. The system might not work as intended on the end devices due to device requirements. 2. The server potentially crashes and essential data is lost. 3. The app might face performance issues due to malfunctions of Firebase APIs. 4. The Version Control System in use might experience fallacies.
2.	People	1. The key people working on the

		project might leave the project. 2. The people working on the project might fall ill and would not be able to work for a period of time. 3. The developer team experiences domain knowledge inadequacies. 4. The team lacks motivation to complete deliverables.
3.	Organizational	1. The organization might be restructured causing a change in the people responsible for different components that might lead to confusion. 2. The project might introduce contract-based members, who can affect team communication and morale.
4.	Tools	1. The final code generated by the SDK might not meet the required performance requirements. 2. Possibility of a single point of failure like loss of all the data that might severely affect the timeline of the project.

		3. The deployment servers might not be scalable enough to meet the demands of peak user traffic.
5.	Requirements Elicitation	1. There might be changes requested by the stakeholders at a later stage of the software development cycle. 2. There might be a difference in the functional requirements documented and functional requirements developed.
6.	Budget	1. The initial budget proposed might not be sufficient to cover additional unforeseen expenditures.
7.	Estimation	1. The time taken to finish a deliverable is underestimated. 2. The number of users in the system might be wrongly estimated. This might impact the design decisions badly. 3. The amount of resources required for the completion of a component is underestimated. 4. The rate of bugs and issues in the system might be

		underestimated.

2.3 RISK ANALYSIS

All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored. Risk Analysis involves identification and assessment of the probability and seriousness of each risk based on consideration of several contributing factors. Probability may be classified into three categories of low, moderate, or high for analyzing the associated risk, depending on the likelihood of the risk. Similarly risk effects can be bifurcated into low, medium, and high, depending on the severeness of the consequences of the risk.

2.3.1 Qualitative Risk Analysis

The agreement of risk level would be brought up by experienced team members and agreed collectively by the team. The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach: The following Impact-Probability matrix will aid in assessing the likelihood and consequences of the risks.

	High	*1. Server Crash* *2. Non-scalable deployment servers* *3. Device requirement not fulfilled* *4. Inefficient Code* *5.Underestimation of Project Size*	*1. Reused Software Component Issues* *2. High Rate of bugs & issues* *3. Version Control fallacies.*	

Impact				
	Medium	*1. Database Limits* *2. API Malfunction* *3. Developer Management Conflict* *4. Undermined Motivation* *5. Project Restructure* *6. Inadequate Domain Knowledge* *7.Abandonment in high pressure* *8. Under/Over Estimation of user base*	*1. Requirement Changes* *2. New use cases* *3. Time Underestimation* *4.Client miscommunication* *5. Team member illness* *6. Single point of failure (e.g., data loss) affecting project timeline* *7. Difference in Functional Requirements documented and deployed.*	
	Low	*1. Project Management Restructure* *2. Contract-based employee affecting team comms.*	*1. Dorm housing structural revamp.*	
		Low	**Medium**	**High**
		Probability		

Fig. 1 Impact-Probability Matrix for RoomieLah!

Probability

· **High** – Greater than **70%** probability of occurrence

· **Medium** – Between **30%** and **70%** probability of occurrence

· **Low** – Below **30%** probability of occurrence

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

Risks that fall within the RED and YELLOW zones will have risk response planning which may include both a risk mitigation and a risk contingency plan. Below is a table classifying the likelihood and seriousness of the consequences of each risk.

S. No	Risk	Probability	Impact
1.	**TECHNOLOGY**		
1.1	The system might not work as intended on the end devices due to device requirements.	**Low**	**High**
1.2	The server potentially crashes, and essential data is lost.	**Low**	**High**
1.3	Firebase API malfunctions	**Low**	**Medium**
1.4	The Version Control System in use might experience fallacies.	**Medium**	**High**
2.	**PEOPLE**		

2.1.	The key people working on the project might leave the project.	**Medium**	**Medium**
2.2.	Conflicts between the developers and project manager	**Low**	**Medium**
2.3.	The people working on the project might fall ill and would not be able to work for a period of time.	**Medium**	**Medium**
2.4.	The team lacks motivation to complete deliverables.	**Low**	**Low**
2.5.	The developer team experiences domain knowledge inadequacies.	**Low**	**Medium**
3.	**ORGANIZATIONAL**		
3.1.	The organization might be restructured causing a change in the people responsible for different components that might lead to confusion.	**Low**	**Low**
3.2.	The project might introduce contract-based members, who can affect team communication and morale.	**Low**	**Low**

4.	**TOOLS**		
4.1.	The final code generated by the SDK might not meet the required performance requirements.	**Low**	**High**
4.2.	Possibility of a single point of failure like loss of all the data that might severely affect the timeline of the project.	**Medium**	**Medium**
4.3.	The deployment servers might not be scalable enough to meet the demands of peak user traffic	**Low**	**High**
5.	**REQUIREMENTS ELICITATION**		
5.1.	There might be changes requested by the stakeholders at a later stage of the software development cycle.	**Medium**	**Medium**
5.2.	There might be a difference in the functional requirements documented and functional requirements developed.	**Medium**	**Medium**
6.	**BUDGET**		

6.1	Budget allocated for the project might not be sufficient to cover additional expenses.	**Medium**	**Medium**
7.	**ESTIMATION**		
7.1.	The time taken to finish a deliverable is underestimated.	**Medium**	**Medium**
7.2.	The rate of bugs and issues in the system might be underestimated	**Medium**	**High**
7.3.	The amount of resources required for the completion of a component is underestimated.	**Low**	**High**
7.4.	The number of users in the system might be wrongly estimated. This might impact the design decisions badly.	**Low**	**Medium**

Table 2: Risk Analysis for RoomieLah!

2.3.2 Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk, and then documented in this section of the risk management plan.

Area of Risk	Severity	Likelihood	Level of Control	Significance
Technology	3	2	2	**7**
People	3	2	2	**7**
Organizational	2	1	2	**5**
Tools	2	1	2	**5**
Requirements Elicitation	3	3	1	**7**
Budget	3	3	1	**7**
Estimation	2	3	2	**7**

Table 3: Quantitative Risk Analysis for RoomieLah!

2.4 RISK RESPONSE PLANNING

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not "fall through the cracks".

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc.

For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

Area of Risk	Chosen Approach	Strategy Description
Organizational	Accept	Any organizational changes that take place will have to be accepted by the team and necessary changes should be made such that the software product and its quality is not affected.
People	Mitigate	To prevent this risk, overall team wellness and cohesion needs to be upheld using team-bonding activities. Overlap in working hours and break hours also help mitigate this risk. It will also ensure substitutability incase of staff illness.
Technology	Avoid	To avoid this risk, sufficient time has to be invested to find the most appropriate technology stacks to be used such that it provides robustness. Investment in highly reliable and scalable databases, cloud services and other such services has to be made to eliminate the possibility of this risk.
Tools	Mitigate	In depth analysis needs to be made and team consensus should be reached before incorporating/using any tool in the project. Even a slightly defective tool should not be used and should be replaced with

		reliable substitutes.
Budget	Accept	Any changes made in the budget mid-way must be accepted by the team unless it becomes completely unviable upon which a meeting with the management is necessary.
Requirements Elicitation	Accept	The requirements of the software may be changed by the relevant shareholders and will have to be accepted by the team. This might result in amendments to the project timeline and other such documents.
Estimation	Mitigate	Sound logical consensus of the team should be present before estimating any part of the project - timeline, milestones, etc.
Other Hazards	Transfer	An outside insurance agency will be made responsible for this risk as the team cannot deal or handle this type of risk.

Table : Risk Response Planning for RoomieLah

2.5 RISK MONITORING, CONTROLLING, AND REPORTING

The level of risk on a project will be tracked, monitored and reported throughout the project lifecycle.
A “Top 10 Risk List” will be maintained by the project team and will be reported as a component of the project status reporting process for this project.
All project change requests will be analyzed for their possible impact to the project risks.
Management will be notified of important changes to risk status as a component to the Executive Project Status Report.

3 TOOLS AND PRACTICES

A Risk Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

Constant monitoring of each risk on a weekly basis will be done and checked by the project manager to ensure everything is in control.

Any risk indicators for each risk will be closely monitored

Risk mitigation strategies will be diligently practiced with frequent reviews and drills to avert any possible risk which may occur during the project

All the identified risks will be reviewed at each team meeting and further updates will be made in case of any new risk

RISK MANAGEMENT PLAN APPROVAL

The undersigned acknowledge they have reviewed the **Risk Management Plan** for the RoomieLah project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature:		Date:	15/03/2022
Print Name:	Srishti Arora		
Title:	Mrs		
Role:	Product Manager		

Signature:		Date:	15/03/2022
Print Name:	Atul Acharya		
Title:	Mr		
Role:	Quality Assurance Manager		

Signature:		Date:	15/03/2022
Print Name:	Aks Tayal		
Title:	Mr		
Role:	Quality Assurance Engineer		

APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
RoomieLah Project Systems Requirements Specification	The RoomieLah Software Systems Requirements Specifications is a detailed document describing all the requirement specifications that this Risk Management Plan refers to	https://github.com/tayalaks2001/roomie_lah/blob/main/Docs/Quality_Plan.pdf
RoomieLah Quality Management Plan	The RoomieLah Quality Management Plan is a detailed document describing all the Quality Assurance (QA) and management protocols which complement the Risk Management Plan	https://github.com/tayalaks2001/roomie_lah/blob/main/Docs/System%20Requirement%20Specifications.pdf

APPENDIX B: KEY TERMS

The following table provides definitions for terms relevant to the Risk Management Plan.

Term	Definition
Budget	The approved estimate for the project or any work breakdown structure component or any schedule activity.
Change Request	A request to expand or reduce the project scope, modify policies, processes, plans or procedures, modify costs or budgets, or revise schedules. Requests for a change can be direct or indirect, externally or internally initiated and legally or contractually mandated or optional. Only formally documented requested changes are processed and only approved change requests are implemented.
Qualitative Analysis	It assesses priority identified by using the probability of occurring and their corresponding impact on project objectives, as well as other factors such as the time frame and risk tolerance of the project constraints of cost, schedule, scope, and quality.
Risk Response Planning	The process of developing options and actions to enhance opportunities and to reduce threats to project objectives. Risk response actions may include mitigations, contingency, transfer, avoidance and acceptance.