

---

***WANDERERS***

**RISK MANAGEMENT PLAN**

---

Version *<1.2>*

*<12/03/2025>*

---

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Kim Seo Jin	01/03/25	Kim Seo Jin	01/03/25	Initial Risk Management Plan draft
1.1	Kim Seo Jin	12/03/25	Kim Seo Jin	12/03/25	Added more detail and adjustments
1.2	Isaac Chun Jun Heng	12/03/25	Isaac Chun Jun Heng	12/03/25	Refined document and added risk matrix

UP Template Version: 12/03/25

# TABLE OF CONTENTS

<b>1 INTRODUCTION.....</b>	<b>4</b>
1.1 Purpose Of The Risk Management Plan .....	4
<b>2 RISK MANAGEMENT PROCEDURE .....</b>	<b>4</b>
2.1 Process.....	4
2.2 Risk Identification .....	4
2.3 Risk Analysis.....	2
2.3.1 Qualitative Risk Analysis .....	2
2.3.2 Quantitative Risk Analysis .....	4
2.4 Risk Response Planning .....	6
2.5 Risk Monitoring, Controlling, And Reporting .....	7
<b>3 TOOLS AND PRACTICES .....</b>	<b>9</b>
<b>RISK MANAGEMENT PLAN APPROVAL .....</b>	<b>10</b>
<b>APPENDIX A: REFERENCES.....</b>	<b>12</b>
<b>APPENDIX B: KEY TERMS .....</b>	<b>12</b>

# 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 *Wanderers* 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 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. **The Project Manager and the Quality Assurance Manager** will serve as the Risk Manager for this project.

### 2.2 RISK IDENTIFICATION

Risk identification will involve the project team, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope. Careful attention will be given to the project deliverables, assumptions, constraints, WBS, cost/effort estimates, resource plan, and other key project documents.

A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library located at **the Wanderers GitHub repo as a risk log artifact**.

The following table highlights some of the risks that we have identified when developing the **Wanderers** project.

Category	Risk
Technical	<ul style="list-style-type: none"><li>• Integration issues with external APIs like Google Places due to rate limits or schema updates.</li><li>• Real-time synchronization failures between users (due to latency, network issues, or database locking).</li></ul>
Financial	<ul style="list-style-type: none"><li>• Budget overrun due to unexpected circumstances.</li><li>• Withdrawal of funds from stakeholders.</li></ul>
Security	<ul style="list-style-type: none"><li>• Data breaches or leaks due to insufficient encryption or misconfigured Supabase storage.</li><li>• Security Misconfiguration (e.g., Supabase rules accidentally left open)</li><li>• Lack of authentication when accessing Wanderers services</li></ul>
Structure/Process	<ul style="list-style-type: none"><li>• Delays due to the following factors:<ul style="list-style-type: none"><li>○ Unclear requirements</li><li>○ Scope creep</li><li>○ Miscommunication within the team</li><li>○ External dependencies</li></ul></li></ul>
Quality	<ul style="list-style-type: none"><li>• Unidentified production bugs and failures due to insufficient testing.</li></ul>
People	<ul style="list-style-type: none"><li>• Team member unavailability due to illness or personal commitments.</li><li>• Team member lack of motivation</li></ul>

	<ul style="list-style-type: none"> <li>Team member resignation or turnover</li> </ul>
Market	<ul style="list-style-type: none"> <li>Strong competitors like TripAdvisor or Google Travel, introducing difficulty in gaining traction.</li> </ul>

## 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.

### 2.3.1 Qualitative Risk Analysis

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:

#### 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

I m p a c t	H			
	M			
	L			
		L	M	H
Probability				

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.

<b>Risk</b>	<b>Probability (%)</b>	<b>Impact</b>	<b>Risk Matrix Color</b>
Insufficient Testing	70% (High)	High	Red
Real-time synchronization failures	50% (Medium)	High	Red
Data breaches or leaks	50% (Medium)	High	Red
Scope Creep	45% (Medium)	High	Red
Integration issues with external APIs (Google Places)	20% (Low)	High	Yellow
Team member unavailability	10% (Low)	Medium	Green
Poor User Experience	10% (Low)	Medium	Green
Security Misconfiguration	30% (Medium)	High	Red
Data Availability Issues	25% (Low)	Medium	Green
Unsatisfactory Performance	30% (Medium)	Medium	Yellow

The following is the **risk matrix** plotted out based on the contents mentioned above:

		Integration issues with external APIs (Google Places)	Real-time synchronization failures Data breaches or leaks Scope Creep Security Misconfiguration	Insufficient Testing
H				
I		Team member unavailability Poor User Experience Data Availability Issues	Unsatisfactory Performance	
m				
p				
a				
c				
t	M			
L				
	L		M	H
		Probability		

From the above-mentioned risks, the following would require a **risk mitigation and risk contingency plan**.

1. Integration issues with external APIs (Google Places)
2. Unsatisfactory Performance
3. Real-time synchronization failures
4. Data breaches or leaks
5. Scope Creep
6. Security Misconfiguration
7. Insufficient Testing
8. Unsatisfactory Performance.

### 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 based on this analysis and then documented in this section of the risk management plan.

#### Probability Rating

- High = 3
- Medium = 2
- Low = 1



### **Severity Rating**

- High = 3
- Medium = 2
- Low = 1

### **Risk Numeric Rating = Probability Rating + Severity**

- 2 & 3 = Low Risk
- 4 = Medium Risk
- 5 & 6 = High Risk

<b>Risk</b>	<b>Probability Rating</b>	<b>Severity Rating</b>	<b>Risk Numeric Rating</b>	<b>Risk Level</b>
Insufficient Testing	3	3	6	High
Real-time synchronization failures	2	3	5	High
Data breaches or leaks	2	3	5	High
Scope creep (unclear requirements)	2	3	5	High
Integration issues with external APIs (Google Places)	1	3	4	Medium
Team member unavailability	1	2	3	Low
Poor user experience	1	2	3	Low
Security Misconfiguration	2	3	5	High
Data Availability Issues	2	2	4	Medium
Unsatisfactory Performance	2	2	4	Medium

## 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.

## 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.

Risk Event	Rank This Month	Rank Last Month	Number of Months in Top 10	Risk Resolution Progress
Insufficient testing	1	2	4	Increased focus on test automation, mandatory code reviews, and enforced test coverage threshold in CI pipeline
Real-time synchronization failures	2	1	4	Enhanced backend retry mechanisms, introduced event queue logging, and planned additional load testing

Data breaches or leaks	3	3	4	Conduct regular penetration testing, stricter Supabase configuration, and review of all data encryption practices
Scope creep	4	4	4	Weekly scope review meetings with sponsors, strict change request process implemented, scrum agile meetings
Integration issues with external APIs (Google Places)	5	5	3	Add secondary API fallback options, reviewed Places API quotas, and limited unnecessary calls
Team member unavailability	6	6	3	Maintained skill redundancy across team, assigned critical tasks to paired developers
Poor user experience	7	7	2	Started regular usability testing with target users, planned design review workshop
Security Misconfiguration	8	8	3	Implemented stricter Supabase rule checks, added weekly security review, and enabled automated alerts for risky configurations
Data Availability Issues	9	9	3	Added periodic data consistency checks, enhanced backup procedures, and included data recovery drills in testing cycles

Unsatisfactory Performance	10	10	3	Conduct regular review of coding output of developers by going through a mandatory process to ensure work is up to standard.
-------------------------------	----	----	---	--

### 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.

## RISK MANAGEMENT PLAN APPROVAL

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

Signature: ICJH Date: 12/03/25

Print Name: Isaac Chun Jun Heng

Title: Quality Manager + Release Manager

Role:

Signature: KSJ Date: 04/03/25

Print Name: Kim Seo Jin

Title: Project Manager

Role:

Signature: YZHA Date: 12/03/25

Print Name: Yu Zi Hao Albert

Title: Development Team Lead

Role:

Signature: JOJX Date: 12/03/25

Print Name: J'sen Ong Jia Xuan

Title: Front-end Developer

Role:



## APPENDIX A: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name and Version	Description	Location
<i>Risk Management Log v1.0</i>	<i>Excel sheet documenting the risk identified for the Wanderers project, its triggers, responses, strategy, etc/</i>	<i>./Risk_Management_Log</i>
<i>Risk Contingency Plan v1.0</i>	<i>This document highlights the plans the team intends to take in the event a risk appears.</i>	<i>./Risk_Contingency_Plan</i>

## APPENDIX B: KEY TERMS

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

Term	Definition
Risk	An uncertain event or condition that, if it occurs, has a positive or negative impact on one or more project objectives.
Probability	The likelihood of a risk occurring, expressed as High, Medium, or Low.
Impact	The severity of consequences if the risk occurs, expressed as High, Medium, or Low.
Risk Matrix	A tool to evaluate and prioritize risks based on their probability and impact.



Risk Response	Actions taken to reduce the probability and/or impact of a risk (e.g., Avoid, Mitigate, Accept, Transfer).
Risk Owner	The team member responsible for monitoring and managing a specific risk.
Qualitative Risk Analysis	Subjective assessment of risks to prioritize them based on probability and impact.
Quantitative Risk Analysis	Numerical assessment of risks to estimate financial and schedule impacts.
Risk Management Plan	Document describing how risks will be identified, analyzed, responded to, and monitored throughout the project lifecycle.
Mitigation Plan	Actions planned to reduce the probability or impact of a risk before it occurs.
Contingency Plan	Actions planned to reduce the impact if the risk actually occurs.
Risk Log	A document or system that records identified risks, their status, owners, and responses.