

A dark blue vertical bar on the left side of the page. A blue arrow points to the right from the bar, containing the date 3/7/2017.

3/7/2017

Risk Management Plan

EXIT6 – Trip Planning Application
for Singapore

Delivered by,

EXIT6 Team

Sim Long Siang(U1522053H)

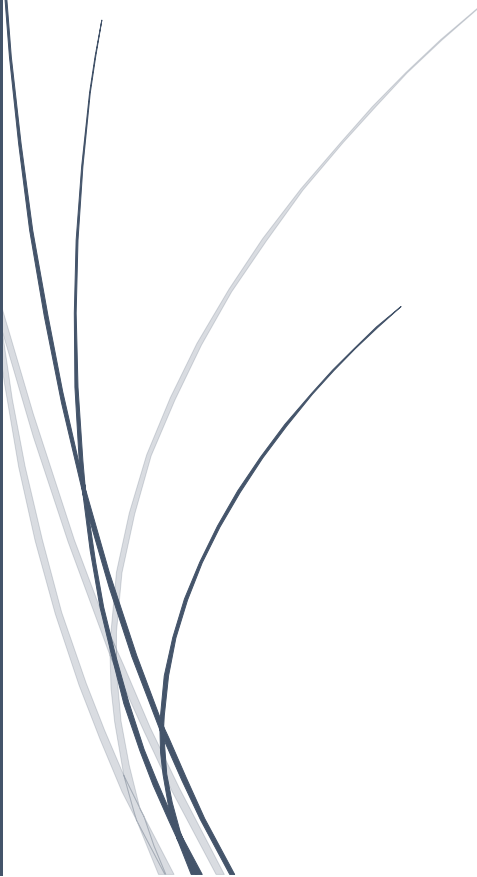
Seshadri Madhavan (U1322790J)

Huang Jian Wei(U1521567A)

Lim Zi Yang(U1522218E)

Lim Hao Zhe(U1521589B)

Tan Jun Qiu(U1321638C)

Several thin, curved lines in shades of blue and grey originate from the bottom left and sweep upwards and to the right, creating a dynamic, abstract design element.

Document Change Record

Revision	Description of Change	Approved by	Date
0.1.0	Initial Template	Tan Jun Qiu	06/02/17
0.5.0	First Draft	EXIT 6 Team	15/02/17
1.0.0	Release	Seshadri Madhavan	07/03/17

Contents

List of Tables	2
Introduction	3
Intended Audience	3
Risk Identification	3
Technological Risk	4
Human Resource Risk/People Management Risk	4
Organizational Risk	5
Tool Risk	5
Requirement Risk	5
Estimation Risk	5
Risk Analysis	6
Overview	6
Risk Planning	8
Risk Monitoring	9
Risk Control	9
Risk Documentation in Risk Log	10
Risk Log	11

List of Tables

Table 1 Probability Classification	6
Table 2 Risk Severity Classification	6
Table 3 Risks Identified and their Effects	7
Table 4 Risk Planning Strategies	8
Table 5 Risk Monitoring Strategies	9

Introduction

This report provides a detailed description of the risk management activities that our group has and will perform to ensure that the EXIT6 application will minimally impacted by risks identified. The purpose of this report is to ensure that the team comes to a consensus regarding various key concepts of risk management that can be encountered during the planning process of developing our EXIT6 application

EXIT6 is an android trip recommendation application that is aimed towards tourists visiting Singapore by generating a unique recommended itinerary based on the user's interests.

The project is handled by a group of NTU students and overseen by Prof. Shen Zhiqi.

Intended Audience

As the purpose of this plan is to provide a common sense of understanding for all the members of the team, the key intended audience for this document are the following personnel:

1. Project Manager, who is in-charge of all the decisions involving the risks in the project
2. QA Manager and QA Engineer, who are responsible to test the integrity of the application being built.
3. Development Team, which is responsible for maintaining and developing the source code that affects the data and system integrity.

Risk Identification

The following sub-categories of the risk are being studied in detail in this document:

1. Technological Risk
2. Human Resource Management Risk/People Risk
3. Organizational Risk
4. Tool Risk
5. Requirement Risk
6. Estimation Risk

Technological Risk

Our application server would primarily be based on NTU's servers given that we plan to host our application on a server that NTU provides. There is a risk that the server would be unable to process many transactions in a short timeframe but this risk is less serious as expected given the robust history of excellence that NTU servers are known to have in the industry.

Additionally, since we do not expect a huge influx of users from the release of our application, the risk of an overload of transactions on the server can be low.

Since the EXIT6 application generates recommended itineraries through computer algorithms, the recommended itineraries may take a longer time to compute should the user provides conditions that result in a high number of possible itineraries which could possibly lead to reduced performance. The risk of such an event happening can be minimized through the decision of limiting the maximum days of a recommended itinerary to be generated to that of 3 days

Software components that should be reused could contain possible defect that limit their functionality but during development, our development team will attempt to avoid reusing software components.

Human Resource Risk/People Management Risk

The EXIT6 application would be planned, developed and released by our own team of NTU students. During this process, there would be limited change or choice of personnel given that groups formed are limited to the pool of people registered to a tutorial group. Therefore, there are possible people risks involved such as the inability to recruit members with the skills required as well as the unavailable of required training provided to the members prior to forming the team.

Despite having access to the internet and lecture notes to provide relevant information, there still exist the risk that members may have a lack of expertise areas of the project

Project members may consist of Final Year Students whom may have other pressing priorities such as their Final Year Project deliverables and meetings which may result in them being absent for certain project meetings. Similarly, project members may also run the risk of falling

ill and become unavailable during critical phases of the project which could potentially slow down project progress.

Organizational Risk

The team organization consist of a group of 6 students whom each had specific roles to play in the team. Since the organization size is small, there is minimal risk that an organizational restructuring could cause a different management to take charge of the project. Project budget would be unlikely to be affected by organizational financial problems as the risk of such financial problems are low.

Tool Risk

The CASE tools primarily used are Android Studio for android application development and Eclipse Mars with Maven Integration for server side development. The code generated by the CASE tools are capable of integration so the risk of tools being unable to integrate is low.

Requirement Risk

Project requirements were primarily elicited by our own team as well as inputs from other surveys with regards to *Trip planning*. Given the scope and the timeframe of the project, there is little risk that changes in requirements that would lead to major redesign issues would occur. Major reworks due to requirement changes are unlikely to occur as the team would have conducted the necessary market research and requirements elicitation procedures before starting on the project.

There is a risk that our customers could fail to understand the impact of requirement changes since our target customers are not easily available for discussion which could lead to a scenario where the they might fail to understand the impact of requirement changes made.

Estimation Risk

Since most of members of the team have limited experience in project management and software development, there lies a moderate risk of us in underestimation of various processes within the project development cycle which can include underestimation of the time required to develop the software, the rate at which defect repair is estimated and as well the number of lines of code estimated to code the software.

Risk Analysis

Overview

After identifying the potential risks, the next step is to analyze the risks. Risk analysis includes estimating the probability of the risk occurring and the severity of the impact in case the identified risk occurs. The estimation can be qualitative or quantitative. This process will translate the risk information to a decision enabling knowledge by doing evaluation. Probability of occurrence can be classified into *Very Low*, *Low*, *Moderate*, *High* or *Very High*. In this project, we will define the probability of occurrence of risk in *Table* as follows:

Table 1 Probability Classification

Risk Classification	Probability	Description
Very Low	<0.01	A situation very unlikely to occur
Low	0.01~0.25	Situation less likely to occur
Moderate	0.25~0.75	Situation may occur
High	0.75~0.90	Situation expected to occur
Very High	>0.90	Situation is highly likely to occur

The severity of the proposed risks can be classified into different types, *namely Insignificant, Tolerable, Serious and Catastrophic*. The meaning of each of the severity is as mentioned below:

Table 2 Risk Severity Classification

Classification	Description
Insignificant	Only very demanding applications are affected
Tolerable	There would be sacrifices in the quality of the core functionalities

Serious	There would be serious hindrances in the quality of the core functionalities
Catastrophic	The entire product will become non-functional and the product may not be delivered on time.

Based on the above defined parameters for the classification of the risks, the following table is being populated for the EXIT6 Trip Planning Application.

Table 3 Risks Identified and their Effects

Risk	Probability	Effects
The database used in the system cannot process as many transactions in a short timeframe	Moderate	Serious
Recommended Itineraries generated by the		
Software components that should be reused contain defects which limit their functionality.	Moderate	Serious
It is impossible to recruit staff with the skills required for the project.	Very High	Tolerable
Required training for staff is not available.	Very High	Tolerable
Key team members are ill at critical times in the project	Moderate	Tolerable
The organisation is restructured so that different management are responsible for the project.	Low	Serious
Organisational financial problems force reductions in the project budget.	Very Low	Insignificant
CASE tools cannot be integrated	Low	Catastrophic
The code generated by CASE tools is inefficient	Moderate	Tolerable
Changes to requirements that require major design rework are proposed.	Low	Catastrophic

Customers fail to understand the impact of requirements changes.	Moderate	Catastrophic
The time required to develop the software is underestimated	Moderate	Serious
The rate of defect repair is underestimated.	Moderate	Serious
The size of the software is underestimated	Moderate	Serious

From the table above, we can infer that most of the risks to take note of related towards the topic of human resource, estimation, technological and tools risk. While the other risks do still matter, there should be more emphasis on the important risk that have both high probability and catastrophic effects.

Risk Planning

Table 4 Risk Planning Strategies

Risk	Strategy
Database performance	<u>Contingency</u> Investigate the possibility of buying a higher performance database should the current NTU server not suffice. Other potential web hosting services such as purchases of Amazon's web services will be taken into consideration should the NTU server not prove to be sufficient.
Software component defects	<u>Avoidance</u> All commonly used components will undergo strict functionality checks to ensure that there are no errors and bugs.
Human resource problems	<u>Minimisation</u> Since this risk is largely unavoidable, our team would have to engage in self learning and collaboration to bridge the knowledge gap
Member illness	<u>Avoidance</u> Organise the team such that there is more overlap of work and members understand each other's jobs such that should one team member fall ill, the other team members are able to pick up the slack
Underestimated development time	<u>Contingency</u> Should there be an overrun in the development schedule, we will consider hiring more developers to ensure that the development schedule can be achieved.
CASE tools integration	<u>Avoidance</u> Before development, research will be conducted to ensure that CASE tools planned to be used during development are capable of integration.

Risk Monitoring

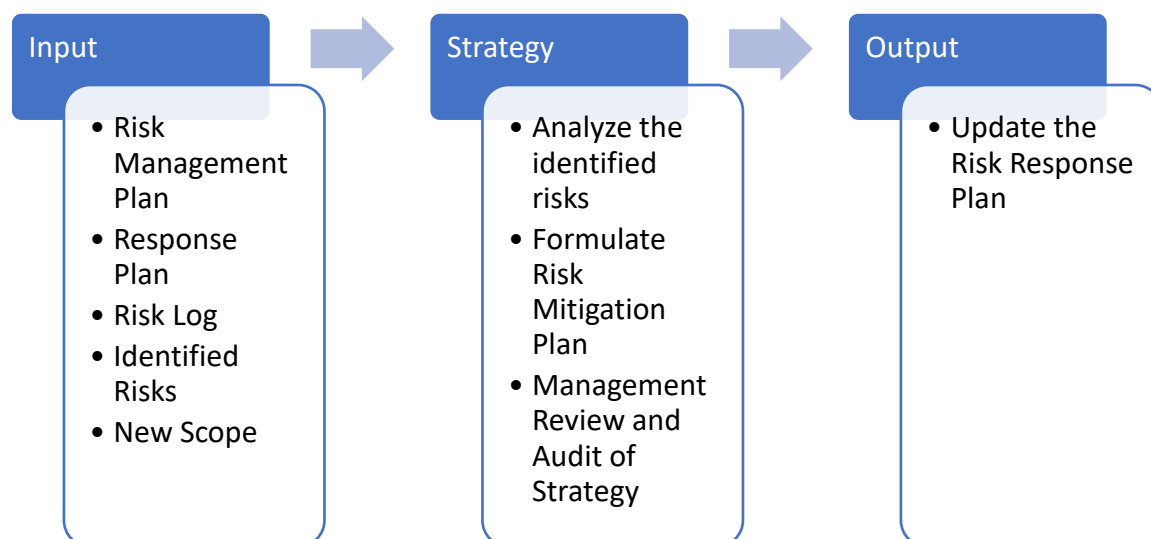
For risk Monitoring, following risks and their proposed indicators are mentioned in the table below.

Table 5 Risk Monitoring Strategies

Risk	Potential Indicators
Database performance	Speed at which database transactions are conducted, reported server errors
Software component defects	Frequent errors when implementing these fundamental software components.
Human resource problems	Poor team morale, members are unwillingly to turn up for team meetings
Underestimated development time	Failure to meet agreed schedule, failure to clear reported defects
Requirements	Development team keeps questioning the need for certain functions that pertain to elicited requirements
CASE tools integration	Complaints about integration using CASE tools

Risk Control

Risk Control involves choosing alternative strategies when risks occur and implementing a contingency plan for the same. The contingency plan must be tested and validated for effectiveness during the use in our project.



Risk Documentation in Risk Log

The results of the Risk Monitoring Process must be documented in the Risk Log as follows:

- Status of active Risks
 - Triggered – Risk has been identified in the current system
 - Resolved – Realized risk has been mitigated but requires monitoring
 - Retired – The risk no longer requires active monitoring
- Risk Management Plan
- Risk Log
- Audit of Risk Management Process

Risk Log

Table 6 Risk Log Table

Risk Type	Risk Description	Probability of Occurrence	Severity	Priority	Mitigation	Status
Technology	Poor Database performance	Medium	Serious	High	Use alternative server	Retired
Technology	Software component defects	Medium	Serious	High	Run strict Functionality checks	Triggered
Technology	Recommended Itineraries are not generated quickly	High	Serious	High	Reduce the complexities of input (limit no of days)	Triggered
People	Team members have inadequate skills	High	Serious	Medium	Online resources and guides	Resolved
People	Training not available for team members	High	Medium	Low	Online resources and guides	Resolved
People	Key members fall ill	Medium	Low	Low	Workload shared between remaining members	Retired
People	Underestimated development time	High	High	High	Leader to keep track of Project Schedule	Triggered
People	Restructuring of organisation	Low	High	Low	Affected members to pass on knowledge to members inheriting their roles	Retired

Requirements	Changes to requirements proposed	Medium	High	High	Proper requirements elicitation done in the first place	Retired
Tools	Problems with CASE tools integration	Low	Catastrophic	High	Conduct integration tests before choosing CASE Tools	Retired