RISK MANAGEMENT PLAN

GuessWho!

Face-Name Matching Game for Dementia Patients

Delivered by:
Bookies
Joshi Chaitanya Krishna(U1522971F)
Genevieve Lam Wen Qi (U1521863H)
Sharma Vidur (U1522940D)
Yong Chen Feng (U1620913B)
Heng Zhi Guang (U1620660F)
Cheng Guanyu (U1621093D)

Submitted to –
Dr Althea Liang
Nanyang Technological University
School of Computer Science and Engineering

Revision History

Version Number	Date	Author(s)	Comments
1.0	16 October 2018	Team Bookies	Initial Version

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this document is to identify the potential risks that the might encounter during the development of the GuessWho! Web Application. A risk is an uncertain event or condition that may likely pose a negative impact to the project, whether it is decreased quality, increased cost, delayed completion, or project failure. Hence, strategies and plans should be put in place to avoid the risk situation or to minimize the effect of the risk on the project.

Project risks can affect project schedule, resources as well as quality of product that the team is developing. Early detection of risks will allow the team to craft plans to avoid or mitigate the anticipated risks. Contingency plans can also be crafted to handle situation where avoidance and mitigation strategy fails.

1.2 Intended Audience

As the purpose of the plan is to provide a common sense of understanding for all team members, the intended audience of this plan includes:

- Project Manager, who is the person in-charge of all decisions involving risk in the project.
- QA Manager and Engineer, who tests the integrity of the application.
- Development Team, which maintains and develops source code that affects system and data integrity.

1.3 Risk Management Process

To successfully manage risks that might the team may encounter during the project, the following steps will be taken to ensure risks are identified, analyzed and appropriate plans are crafted to manage the risks. These steps are as follows:

1.3.1 Risk Identification

The Identification of risk can be done by providing a list of potential risks that might affect the project. It should include the details about the risk such as the risk factor, category and description. The identification could be done through methods such as brainstorming, interviews, checklists and scenario analysis

1.3.2 Risk Analysis

Estimate the probability of the risk occurring, the estimation can be qualitative or quantitative. This process will translate the risk information to a decision enabling knowledge by doing evaluation.

1.3.3 Risk Response Planning

After analyzing the risks, the next step is to draw up plans to avoid and minimize the effect of the risk.

1.3.4 Risk Monitoring & Control

Monitoring and control involves implementing procedures and actions to monitor the risks throughout the projects. All risks, especially those of higher priority, will be closely monitored. Corrective actions will be undertaken for the risks should there be a need to do so. Risk monitoring will also seek out new risks throughout the project.

2. Roles and Responsibilities

In order to ensure smooth planning and execution, the risk management tasks will be distributed among the team members as stated in *Table 1* below:

Task	**Responsible Party**
<u>Overall Risk Management Planning</u>	
Overall risk management responsibility	Project Manager
Develop risk management strategies and draft risk management plan	QA Manager & Engineer
Review risk management plan	Team
Approve risk management plan	Project Manager
<u>Risk Identification</u>	
Identify potential risks through situation analysis	QA Manager & Engineer
Document identified risks in Risk Log	QA Manager & Engineer
<u>Risk Analysis</u>	

Analyze probability of occurrence and severity of risks	Project Manager, QA Manager & Engineer
Prioritize risks according to calculated risk levels	Project Manager, QA Manager & Engineer
Review Risk Log	Team
Risk Response Planning	
Develop response plan (including avoidance and mitigation strategy, as well as contingency plans) to handle the risks	Project Manager & QA Manager
Risk Monitoring and Control	
Regularly access identified risks including any change in possibility of occurrence and change in effect	Project Manager, QA Manager & Engineer

3. Risk Identification

3.1 Overview

Risk Identification is a process of determining possible adverse circumstances and situations that can occur during the Software Development Life Cycle. A risk should be classified according to its type and subsequently documented into the Risk Log.

Some risks can be identified and predicted during the initial phase of the project while others are only detected during the development phase of the project. As a result, risk identification is an iterative and ongoing process that consistently reviews project progress to ensure that all risks are identified and solved.

- Risks identified are typically classified into six types – *Technology, People, Organizational, Tools, Requirements* and *Estimation*.
- Technology Risks – Risks that derived from software and hardware technologies that are being used as part of the system that is being developed.
- People Risks – Risks that occur due to team member's availability, skill level, or retention of team member.
- Organizational Risks – Risks that are caused by the environment where the system is being developed.
- Tools Risks – Risks that are related to the availability and reliability of the supporting tools used for the project.
- Requirements Risks – Risks that occur due to change in requirements or lack of understanding of the impact caused by these changes.
- Estimation Risks – Risks that appear from inaccurate estimation of resources and duration required for the project.

The Risk Identification process implemented for this project has been done through brain-storming and analysis of situations. The table below states the risks identified during the development of the

project. The table will also include the risk classification and a description that includes the detail and nature of the risk.

Table 2: *Risk Identification*

	RISK TYPE	RISK DESCRIPTION
1	Technology	Possibility of single point of failure, like data corruption, which can jeopardize the whole project.
2	People	Key team members are unavailable often at critical timings.
3	People	Required training for team members is not available due to time constraint.
4	People	Team members have limited experience in software development.
5	Tools	System might not be able to work as planned on mobile browsers due to development tools constraints.
6	Requirements	Difference between functional requirements documented and functional requirements developed.
7	Requirements	Drastic updates to functional requirements due to development constraints may delay the project schedule.
8	Estimation	Team members' limited experience can set unrealistic timeline for project thus causing a loss of control for project.
9	Estimation	Team members' limited experience and skillset can set unrealistic goals to functional requirements, such as implementing complex features beyond members' skillset.

4. Risk Analysis

4.1 Overview

Risk Analysis is a process that follows Risk Identification process, which estimates the probability of occurrence and the severity of the impact it can cause. The probability can be categorised into *Very Low, Low, Moderate, High* or *Very High,* while the severity of the impact the risks can cause can be categorised into *Catastrophic, Serious, Tolerable,* or *Insignificant*.

Table 3: *Classification of Probability of Occurrence of Risk*

	RISK DESCRIPTION	PROBABILITY	SEVERITY
1	Possibility of single point of failure, like data corruption, which can jeopardize the whole project.	Very Low	Catastrophic
2	Key team members are unavailable often at critical timings.	Low	Tolerable
3	Required training for team members is not available due to time constraint.	Very High	Tolerable
4	Team members have limited experience in software development.	Moderate	Serious
5	System might not be able to work as planned on mobile browsers due to development tools constraints.	Moderate	Tolerable
6	Difference between functional requirements documented and functional requirements developed.	Low	Serious
7	Drastic updates to functional requirements due to development constraints may delay the project schedule.	Low	Catastrophic

8	Team members' limited experience can set unrealistic timeline for project thus causing a loss of control for project.	Very Low	Catastrophic
9	Team members' limited experience and skillset can set unrealistic goals to functional requirements, such as implementing complex features beyond members' skillset.	Low	Serious

5. Risk Response Planning

5.1 Overview

GuessWho! project team is responsible in selecting a risk response for each identified risk. To minimize the impact of each risk, the team has to develop and determine various action to enhance prospects. Risk with greater impact are given greater priority than risks with lesser impact.

5.2 Risk Strategies

Response planning for GuessWho! follows three main strategies: risk avoidance, risk mitigation and contingency planning.

5.2.1 Risk Avoidance

Risk avoidance involves elimination of risk, activities and exposures that can negatively affect the outcome of the project. Its strategy is designed to deflect as many risk as possible in order to avoid the costly and disruptive outcome. Once all risks are identified, it attempts to minimize vulnerabilities which can pose a threat. For example, there a risk in the performance degradation of the picture display when the user has to choose. This risk can be avoided by ensuring all photo size are of the same size.

5.2.2 Risk Mitigation

Risk mitigation is defined as taking steps to reduce adverse effects. However, this does not eliminate risk completely but it can be greatly reduced by making sure that the impact of the risk does not hinder functionality.

5.2.3 Contingency Planning

Certain risks are an inherent part of every project and dealing with them by any means is too cost-inhibitive. These type of risks have to be accepted by the team members, and can be documented and re-evaluated at fixed intervals of time to make sure that their impact has not grown, and a handling method of the risk can be devised instead.

5.3 Documentation

The result of response planning will be documented in the Risk Log in the Appendix. The following information should be recorded:

- Priority (High, Medium, Low)
- Severity (Catastrophic, Serious, Tolerable, Insignificant)
- Occurrence (High, Moderate, Low)
- Mitigation/ Contingency Plan

6. Risk Monitoring and Control

6.1 Risk Monitoring

To combat against existing and new risks, GuessWho! project team conducts the risk monitoring to ensure the plan's execution for risk handling and its effectiveness.

6.2 Risk Control

In several cases, unforeseen risks may occur; thus, an effective contingency plan is required to control the risks. The solution includes alternating between different strategies and implementing the plan as a provision. The effectiveness of the plans is ensured through testing regarding risk handling.

6.3 Documentation

The implementation of risk monitoring and risk control yields many results. The documentation of the results includes:

- Status of active risks
  - ***Triggered:*** Risk trigger has occurred and threat has been realized
  - ***Resolved:*** Realized risk has been contained
  - ***Retired:*** Identified risk no longer requires active monitoring (e.g. risk trigger has passed)
- Risk Management Plan
- Risk Log
- Management Process Audit

Appendix

Risk Log

	RISK TYPE	RISK DESCRIPTION	OCCURRENCE	SEVERITY	PRIORITY	MITIGATION / CONTINGENCY PLAN	STATUS
1	Tools	Possibility of single point of failure, like data corruption, which can jeopardize the whole project.	High	Serious	High	Modularity in programming to create independent units	Retired
2	People	Key team members are unavailable often at critical timings.	High	Serious	High	Research online for tutorial and practices	Resolved
3	People	Required training for team members is not available due to time constraint.	High	Serious	High	Research online for tutorial and practices	Resolved
4	People	Team members have limited experience in software development.	Low	Insignificant	Low	Plan few weeks in advance so that it can accommodate as many people	Resolved
5	Technology	System might not be able to work as planned on mobile browsers due to development tools constraints.	Low	Catastrophic	Medium	Ensure the application is available across different platform	Triggered
6	Requirements	Difference between functional requirements documented and functional requirements developed.	High	Tolerable	Medium	Conduct weekly meetings to review requirements and functionalities	Triggered
7	Requirements	Drastic updates to functional requirements due to development constraints may delay the project schedule.	Moderate	Serious	Medium	Document the updates made in the software	Triggered
8	Estimation	Team members' limited experience can set unrealistic timeline for project thus causing a loss of control for project.	High	Serious	Medium	Implement deadline for each task allocated	Triggered
9	Tools	Team members' limited experience and skillset can set unrealistic goals to functional	High	Serious	High	Ensure the application is available across different platform	Retired

		requirements, such as implementing complex features beyond members' skillset.					

Management Process Audit Template

Improvement Initiative	Action	Responsible Party	Due Date	Achieved	Comments

Management Process Audit