Risk Management Plan

29/09/2014

Stephen Tate

CO600: JustHealth
Supervisor: Yang He

Version 1.1
Last saved by: Ben McGregor
Last saved on: 29/03/2015

Contents

1.0 Introduction

A risk is a possible event that may occur which could cause harm or loss, or affect the ability to achieve project objectives (Farenden, 2011). Risk Management is the process of identifying, analysing, reacting to, monitoring and reporting these events. This risk management plan defines how risks associated with the JustHealth project will be identified, analysed and managed by outlining how the risk management process and activities will be carried out throughout the lifecycle of the project. It will also provide templates and instructions on how to use these templates and processes to appropriately managing project risks.

2.0 Roles and Accountability

Name	Title	Role Responsibility
Stephen Tate	Risk Manager	Responsible for ensuring that identified risks are added to the Risk Management Log and that they are regularly updated with appropriate actions. Any risks that are not able to be assigned to an appropriate person in the project team should be assigned to the risk manager. Also, responsible for identifying risks that have expired and should ensure that they are re-opened where appropriate or closed in the Risk Management Log.
Charlotte Hutchinson	Project Manager	Responsible for ensuring that Risks are reviewed in project team meetings on a regular basis.

3.0 Risk Management Process

Everyone working within the project team is responsible for identifying and subsequently recording risks. It is crucial that risks are identified as soon as possible so that the project team is aware and can plan effectively to minimise the impact of the risk. As a part of their regular meetings, the project team will review the risks and come up with plans to manage the risk effectively and appropriately.

3.1 Risk Identification

Everyone within the project team is responsible for both risk identification and recording the risk. Risks should be recorded in the Risk Management Log and medium/high risks should be assigned to/owned by the most appropriate person within the project team that is working on the area where the risk is exposed; if there is not one person that is clearly accountable then the risk should be assigned to the Risk Manager. Furthermore, risks that are identified should be categorised within the following:

1. People – a lack of skills, understanding, time, resources.
2. Technical – problems with the implementation, technical complexity, limitations of technical components.
3. External Influences – Anything from outside the project and/or project team that may directly affect the work being carried out on the project.
4. Legal – Any legal boundaries/requirements that may pose a risk to the project.

The Risk Management Log will be stored electronically project shared area and should be updated as required.

3.2 Risk Analysis

All risks that are identified by the project team should be assessed collectively and all possible outcomes that are identified should be recorded in the Risk Management Log. The project team will adopt the composite risk index in order to determine high, medium and low risk events.

Composite Risk Index = Impact of Risk Event x Likelihood of Occurrence

Impact of Risk Event

Very Low Impact *Very High Impact*

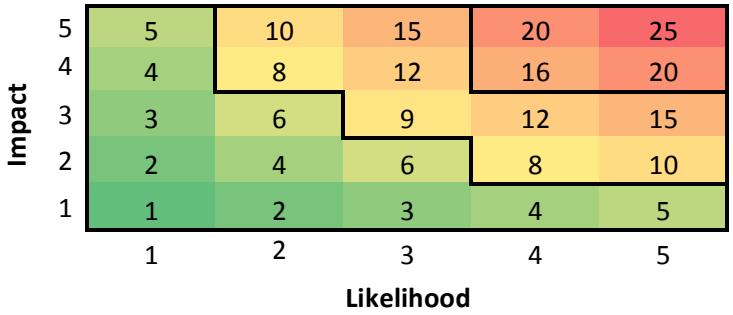
1	2	3	4	5

Likelihood of Risk Event

Very Low Likelihood *Very High Likelihood*

1	2	3	4	5

Result



The result of the composite risk index formula should be recorded in the Risk Management log and subsequently will enable the team to create and manage an appropriate mitigation plan. Risks will be generically categorised into the following:

1. High Risk: 16-25
2. Medium Risk: 7-15
3. Low Risk: 1-6

3.3 Risk Response Planning

Every Medium/High Risk will have an owner assigned, that will be the most appropriate person within the project team that is working on the area where the risk is exposed; if there is not one person that is clearly accountable then the risk should be assigned to the Risk Manager.

As outlined in ISO 27005, one of the following approaches will be assigned and an action plan will then be drawn up and recorded in the Risk Management Log.

1. **Retain** – Accept the risk because there is nothing that is able to be done to reduce or remove the risk.
2. **Transfer** – This would usually entail involving another company that would be responsible for the risk, although may also include building prototypes or adding more steps into the project plan with the intention that these reduce the likeliness or impact of the risk.
3. **Mitigate** – Identify ways to reduce the probability or impact of the risk; this may be to use a different method/technique/process to achieve a particular objective.

4. **Avoid –** This is achieved by eliminating the situation, process or goal which in turn removes the risk that it represents.

3.4 Risk Reporting and Management

All of the risks identified will be reviewed by the project team on a fortnightly basis and high risk items will be reviewed on a weekly basis. The Risk Management Log will be updated with new entries on an ad-hoc basis and will be updated with relevant actions and plans as a part of the meetings when risks are reviewed.

Once the project is concluded the Risk Management Log will be included as an appendix of this Risk Management Plan.