

StarContests.com

If it's not here it's not happening.

***Risk Management, Mitigation and
Monitoring Plan v1.0***

Team 8

Instructor - Prof. Asim Banerjee

Overview:

This Risk Management Plan defines how risks associated with the 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.

Intended Audience:

- Project team
- Client

Document revision History:

Version	Author	Description	Reviewed By	Date
1.0	Rachit Mishra	RM ³ P v1.0	Prachi Kothari	4 th April, 2015

TABLE OF CONTENTS

1.	Introduction ..	4
1.1.	Purpose ..	4
1.2.	Scope ..	4
1.3.	References ..	4
2.	Roles and Responsibilities ..	5
2.1.	Project Manager ..	5
2.2.	Project Team – Team 8 ..	5
2.3.	Client – Viva Des Sportes ..	5
3.	Risk management Procedure ..	6
3.1.	Process ..	6
3.2.	Risk Identification ..	6
3.3.	Risk Analysis ..	7
3.3.1.	Qualitative Risk Analysis ..	7
3.3.2.	Quantitative Risk Analysis ..	9
3.4.	Risk Response Planning ..	10
3.5.	Risk Monitoring, Controlling, And Reporting ..	11

1. Introduction

1.1 Purpose Of The Risk Management Plan

This purpose of Risk Monitoring, Management and Mitigation Plan for the project - Interview Platform is to define the risk management process to be employed throughout the life of this project. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting 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.

1.2 Scope

The scope of this document pertains to the project - Interview Platform and its internal and external risks. The risk management methodology identified in this document will be primarily used by the developing team and is to be used throughout the course of the entire project.

1.3 References

- Software requirements specification v2.0, Team 8 - Interview Platform, IT314 Software Engineering, winter 2012-13, DA-IICT.
- IEEE Standard 1012-1998: IEEE Standard for Software Verification and Validation
- Mertia, Sandeep et. al., Team 7 - Entelechy Website - RMMMP, IT314 Software Engineering, Winter 2012-13, DA-IICT.

2. Roles and Responsibilities

2.1 Project Manager

- Overall responsibility for the risk management process, to ensure that foreseeable risks (both threats and opportunities) are identified and managed effectively and proactively to maintain an acceptable level of risk exposure for the project.
- Write and approve the Project Risk Management Plan, define the Risk Management process, participate in the Risk Management process, and take ownership of risk mitigation planning and execution.
- Determining the acceptable levels of risk for the project by consultation with the Client.

2.2 Project Team – Team 8

- Project team members (product managers, developers, testers, and deployment team members) participate in the risk identification process and discuss risk monitoring and mitigation activities at team meetings.
- Participating actively in the risk process, proactively identifying and managing risks in their area of responsibility.

2.3 Client – Viva Desportes

- Clients participate in risk identification and risk activities, by providing risks input, and supporting risk mitigation planning and execution activities.
- Actively supporting and encouraging the implementation of a formal risk management process on the project.
- Reviewing risks escalated by the Project Manager which are outside the scope or control of the project or which require input or action from outside the project.
- Taking decisions on project strategy in the light of current risk status, to maintain acceptable risk exposure.

3. Risk management Procedure

3.1 Process

The project manager working with the project team and client 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.

3.2 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, cost/effort estimates, resource plan, and other key project documents.

Risk Areas	Risks Identified
Technical Risk	Insufficient knowledge of required software tools
	Firsthand experience of big projects
	Unavailability of technical resources
Project Definition	Underestimation of product size
	Wrong selection of Software Development Life Cycle Model
Project Planning	Difficulty in meeting the deadlines
	Inconsistency in subsequent updates of documents
Customer Characteristics	Difficulty in working with the client due to changes in requirements
	Bad team management and work distribution by the leader

Personnel Risk	Conflicts among team members
Performance Risk	Incompatibility of two modules / plugins
	Website/server crashes

3.3 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.

3.3.1 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

S.No	Risks Identified	Probability	Impact
------	------------------	-------------	--------

1	Insufficient knowledge of required software tools	Medium	High
2	Firsthand experience of big projects	High	High
3	Unavailability of technical resources	Low	High
4	Underestimation of product size	Low	Medium
5	Wrong selection of Software Development Life Cycle Model	Medium	Medium
6	Difficulty in meeting the deadlines	Medium	Medium
7	Inconsistency in subsequent updates of documents	Low	Low
8	Difficulty in working with the client due to changes in requirements	Medium	Low
9	Bad team management and work distribution by the leader	Low	High
10	Conflicts among team members	Low	Medium
11	Incompatibility of two modules / plugins	Medium	Medium
12	Website/server crashes	Low	High

After the risks are prioritized, a risk probability and impact matrix is generated which helps in deciding the relative priority of risks. Risks that fall into:

- Red-shaded cells of the matrix shown below are of the highest priority and should receive a majority of the risk management resources during response planning and risk monitoring and control.
- Risks that fall into the yellow-shaded cells of the matrix are of the next highest priority, followed by the risks that fall into the green-shaded cells.
- The risk probability and impact matrix is as shown below:

Impact	H	3, 9, 12	1	2
	M	4, 10	5, 6, 11	
	L	7	8	
		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.

3.3.2 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.

3.4 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

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.

S.No	Risks	Approach	Mitigation	Contingency
1	Insufficient knowledge of required software tools	Mitigate	Refer books and internet for the technologies to be used	Seek expertise experience in using
2	Firsthand experience of big projects	Mitigate	Working on a task in groups with people experienced in software development	Keep constant check and help fellow team members achieve their goals.
3	Unavailability of technical resources	Mitigate	Prior planning and research of the needed system tools and applications	Look for alternate resources and consider
4	Underestimation of product size	Avoid	Revise the scope of the project very frequently	
5	Wrong selection of Software Development Life Cycle Model	Avoid	Constant check on whether the Life Cycle chosen is being put to utilization	Access the work and determine course thereafter.
6	Difficulty in meeting the deadlines	Mitigate	Keep milestones and verify constantly whether we are up to date	Review of the deadlines and set new deadlines that are realistic keeping in mind all the constraints in the plan.
7	Inconsistency in subsequent updates of documents	Avoid	Regular checking of documents and maintaining the previous versions. Following a documentation standard.	
8	Difficulty in working with the client due to changes in requirements	Mitigate	Understanding the needs of the customer and comply with the changes proposed by them	

9	Bad team management and work distribution by the leader	Avoid	Consulting with team members before taking decisions	Other members part in leadership decisions
10	Conflicts among team members	Avoid	Understanding various viewpoints involved in conflict and resolve them through meetings.	
11	Incompatibility of two modules / plugins	Mitigate	Execute the unit and integration test plans to figure out the error, and resolve it.	Try to find alternative plugins or make code of the given
12	Website/server crashes	Mitigate	Understand the system and network requirements at client and server side before starting implementation.	Contact System Administrator

3.5 Risk Monitoring, Controlling, And Reporting

The objectives of risk monitoring and updating are to:

1. systematically track the identified risks
2. identify any new risks
3. effectively manage the contingency reserve
4. capture lessons learned for future risk assessment and allocation efforts

The risk monitoring and updating process occurs after the risk mitigation, planning, and allocation processes. It must continue for the life of the project because risks are dynamic. The list of risks and associated risk management strategies will likely change as the project matures and new risks develop or anticipated risks disappear.

Periodic project risk reviews repeat the tasks of identification, assessment, analysis, mitigation, planning, and allocation. Regularly scheduled project risk reviews can be used to ensure that project risk is an agenda item at all project development and construction management meetings.

If unanticipated risks emerge or a risk's impact is greater than expected, the planned response or risk allocation may not be adequate. At this point, the project team must perform additional response planning to control the risk.

Risk Status

The risk status assigned to each risk changes over the project's life cycle. The risk statuses are defined as:

Active = risk is being actively monitored

Dormant = risk is not currently high priority, but may become active in the future

Retired = risk has been resolved

S.No	Risks	Status	
1	Insufficient knowledge of required software tools	Dormant	
2	Firsthand experience of big projects	Retired	
3	Unavailability of technical resources	Retired	
4	Underestimation of product size	Dormant	
5	Wrong selection of Software Development Life Cycle Model	Dormant	
6	Difficulty in meeting the deadlines	Active	
7	Inconsistency in subsequent updates of documents	Active	
8	Difficulty in working with the client due to changes in requirements	Dormant	
9	Bad team management and work distribution by the leader	Active	
10	Conflicts among team members	Dormant	
11	Incompatibility of two modules/ plugins	Active	

12	Website/server crashes	Dormant
----	------------------------	---------