IT314 Software Engineering Team 7

Risk Monitoring, Management & Mitigation Plan

Version 1.0

28 March, 2013

Winter 2012-13
DA-IICT, Gandhinagar

Overview:

Risk Monitoring, Mitigation and Management Plan for the new Entelechy website.

Target Audience:

Software Development Team
Clients

Document Revision History:

Version	Primary Author(s)	Description	Reviewed By	Date
1.0	Sandeep	RMMMP v1.0	Abhishek, Nitish	28 March, 2013

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this Risk Monitoring, Management and Mitigation Plan (RMMMP) is to describe the methodology for identifying, tracking, mitigating, and ultimately retiring the risks involved with the project.

It will establish the framework in which the project team will identify risks and develop strategies to mitigate or avoid those risks. The primary purposes of this document are:

- Risk Identification
- Risk Analysis
- Risk Management and Mitigation
- Risk Review and Monitoring

1.2 Scope

The scope of this document pertains to the Entelechy Website Project and its internal and external risks. The risk management methodology identified in this document will be primarily used by Entelechy website and is to be used during the entire project.

1.3 Risk Management Overview

Risks are future uncertain events with a probability of occurrence and a potential for loss or delay. It is an unfavorable event or circumstance that can occur during the project life cycle which can affect the delivery of project in cost and time effective manner. Risk identification and management are the important concerns in the project.

1.3.1 Risk identification

Risks are about events that, when triggered, cause problems. Hence, risk identification can start with the source of problems, or with the problem itself.

- Source analysis: Risk sources may be internal or external to the system that is the target of risk management.
- Problem analysis: Risks are related to the identified threats.

PTO

1.3.2 Risk Analysis

Risk analysis is a set of techniques used to investigate problems created by uncertainty and to assess their effects. Risk analysis assesses the loss probability and loss magnitude for each identified risk. The purpose of risk analysis is to understand risk better and to verify and correct attributes. No software development life cycle is said to be complete unless it has passed through rigorous and active consideration of the several types of risk associated with the development of the software. During risk analysis, the value of opportunities to pursue vs. threats to avoid and the opportunities to ignore vs. threats to accept are assessed. Risk analysis helps in preparing a contingency plan to contain the risk effects. Risk analysis involves assigning each risk with its probability of occurrence and estimating the impact of each risk.

1.3.3 Response Planning

Response planning is aimed at determining options and actions to reduce the likelihood or consequences of risk impact on the project's objectives or progress. During response planning, risk management and contingency plans are developed that describe the action to be taken to mitigate each risk and the action to be taken when this risk event occurs. Response planning also involves assigning responsibilities for each agreed response. Response tracking is maintaining required documents that state necessary conclusions throughout the software development life cycle.

1.3.4 Risk Monitoring and Control

Risk monitoring and control is highly important for avoiding the occurrence of a risk event. It involves the development, implementation and monitoring of corrective action plans that help in avoiding risk.

2. Roles and Responsibilities

2.1 Project Manager – Sandeep

The role of the Project Manager is to 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.

PTO

2.2 Project Team – Team 7

Project team members (analysts/product managers, developers, testers, and deployment team members) participate in the risk identification process and discuss risk monitoring and mitigation activities at team meetings.

2.3 Clients – Press Club, DA-IICT

Clients participate in risk identification and risk activities, by providing risks input, and supporting risk mitigation planning and execution activities. As the project sponsors they also receive escalated risks and assist with mitigation and contingency actions for escalated risks and cultivate a culture that rewards early identification and treatment of risks and issues.

3. Risk Identification

Risk Areas	Risks Identified
Product Size	Uncertain Product Size
Customer Characteristics	Customers/Clients do not understand the exact requirements of their organisation
Customer Characteristics	Customer/Clients may change their requirements
Project Planning	Unrealistic deadlines for deliverables/milestones
Process Definition	Not following the process defined for development
Process Definition	Wrong selection of the Software Development Life Cycle to complete the project in the given time and with the given team members
Requirements	Ambiguity in requirements
Design	Wrong interpretation of SRS in Design
Technical	Lack of experience or training in using software tools and technologies
Technical	Too much complexity involved in WordPress development
Personnel	Unavailability of team members
Personnel	Conflicts among team members
Personnel	Faulty work distribution
Personnel	Bad team management and planning by the leader
Performance	Entelechy website crash
Performance	Incompatibility of two modules/plugins
Performance	DA-IICT server does not work properly

4. Risk Analysis

4.1 Determining Risk Impact

Determining the risk impact considers the consequences the risk would have on the project if the risk event occurs. Risk impact is a description of the anticipated consequences of a risk event occurring impact is a description of the anticipated consequences of a risk event occurring. The Criteria for Risk Impact for evaluating the risk consequences and determining the risk impact, expressed as “low“, “medium,” or “high”.

- High Impact
  - Significant schedule delay. For example, delay in a critical path activity by more than 2 weeks.
  - Significant cost increase. For example, project budget or cost increase by more than 20%.
  - Significant technical change. For example, system performance decreases by more than 30-40%.
  - Significant resource change. For example, loss of more than 30% of personnel.
  - Significant user dissatisfaction. For example, more than 20-30% of users are extremely dissatisfied with more than 20-30% of system functions or performance characteristics.

- Medium Impact
  - Moderate schedule delay. For example, delay in a critical path activity by 1 week, or delay in a non-critical path activity by 2 weeks.
  - Moderate cost increase. For example, project budget increase by 10-20%.
  - Moderate technical change. For example, system performance decreases by 20-30%.
  - Moderate resource change. For example, loss of 20% of personnel.
  - Moderate user dissatisfaction. For example, 10-20% of users are extremely dissatisfied with 10-20% of system functions or performance characteristics, or more than 20% of users are moderately dissatisfied with more than 20% of system functions or performance characteristics.

- Low Impact
  - Minor schedule delay. For example, delay in a critical path activity by less than 1 week, or delay in a non-critical path activity by less than 2 weeks.
  - Minor cost increase. For example, project budget increase by less than 10%.
  - Minor technical change. For example, system performance decreases by less than 20%.
  - Minor resource change. For example, loss of less than 10% of personnel.

- Minor political repercussions. For example, minor dissatisfaction of political parties or special interest groups.
- Minor user dissatisfaction. For example, less than 20% of users are extremely dissatisfied with less than 20% of system functions or performance characteristics.

4.2 Determining Risk Probability

Determining risk probability involves considering the likelihood of the risk occurrence. The criteria for the risk probability are high, medium or low.

- High: It is almost certain or very likely that the risk will occur. There is approximately a 65% or higher confidence level that the risk will occur.
- Medium: It is somewhat probable that the risk will occur. There is approximately a 35-65% confidence level that the risk will occur.
- Low: It is unlikely or improbable that the risk will occur. There is approximately a less than 35% confidence level that the risk will occur.

4.3 Risk Analysis Table

After risks are identified and documented, risk analysis is performed to analyse each potential risk event for:

- Probability of Occurrence
- Impact of the risk event if it occurs

The risk analysis for our project is as follows

S.No.	Risks Identified	Probability	Impact
1	Uncertain Product Size	Low	High
2	Customers/Clients do not understand the exact requirements of their organisation	Low	High
3	Customer/Clients may change their requirements	Low	Medium
4	Unrealistic deadlines for deliverables/milestones	Medium	Medium
5	Not following the process defined for development	Medium	Medium
6	Wrong selection of the Software Development Life Cycle to complete the project in the given time and with the given team members	Low	High
7	Ambiguity in requirements	Low	High
8	Wrong interpretation of SRS in Design	Medium	High
9	Lack of experience or training in using software tools and technologies	High	High
10	Too much complexity involved in WordPress development	High	High

11	Unavailability of team members	Medium	High
12	Conflicts among team members	Low	Low
13	Faulty work distribution	Low	High
14	Bad team management and planning by the leader	Low	High
15	Entelechy website crash	Medium	Low
16	Incompatibility of two modules/plugins	Medium	High
17	DA-IICT server does not work properly	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:

Probability(↓) /Impact (→)	**Low**	**Medium**	**High**
High			**9, 10**
Medium	**15**	**4, 5**	**8, 11, 16**
Low	**12**	**3**	**1, 2, 6, 7, 13, 14, 17**

5. Risk Planning

Risk planning involves assigning risk ownership, developing risk mitigations, contingencies, and translating mitigations into action plans to minimize the impacts of risk to a point where the risk can be controlled and managed. Higher priority risks receive more attention than the lower priority risks.

5.1 Risk Strategies

There could be numerous complicated risk strategies for a software project. The risk strategies which we've adopted are – Prevention, Mitigation and Contingency.

Prevention: Risk prevention involves changing the overall project management plan to avoid the threat. Risks are identified early in the project can be prevented by clarifying requirements, obtaining more detailed information, improving communications or obtaining expertise.

Mitigation: Risk mitigation involves reducing the probability and/or impact of the risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage that a realized risk event has caused.

Contingency: Developing contingency plans helps define the plan of action and strategy to adopt if and when a risk event does occur. It helps in swift and efficient allocation of risk management resources if a risk event occurs.

The risk strategies for our Entelechy Website project are as follows:

S.No.	**Risks**	Prevention	Mitigation	Contingency
1	Uncertain Product Size	Determine the range of the problem size and decide on a realistic scope of project to be implemented.	Have well defined and documented scope of the project to be implemented	Review and decide on the problem size that is realistic.
2	Customers/Clients do not understand the exact requirements of their organisation	Discussion with the clients about their requirements	Proper documentation of clients' requirements	Understanding clients' requirements through by analysing similar organisations or systems, or in case of users – do ethnographic studies
3	Customer/Clients may change their requirements	Discussion with the clients about their requirements	Proper documentation of clients' requirements	Negotiating with the clients to reach best possible solution
4	Unrealistic deadlines for deliverables/milestones	Setting deadlines realistically keeping in mind the tasks at hand and constraints of time and resources	Review of the deadlines set and distributing the tasks effectively for timely completion	Review of the deadlines and set new deadlines that are realistic keeping in mind all the constraints
5	Not following the process defined for development	Have a well-defined process for development	Keeping track of the project's progress and review of the work completed	Reorganizing to bring the project's development process back on track

6	Wrong selection of the Software Development Life Cycle to complete the project in the given time and with the given team members	Proper review and understanding of the pros and cons of each software development life cycle and assessment of the project for the most suitable model when selecting it.	Modification of the software development life cycle model selected to better adopt it for the project's efficient and timely completion	Management and review of the work already completed and determining the course of action for the remaining work to be completed successfully
7	Ambiguity in requirements	Proper – detailed and holistic requirements analysis should be carried out before creating SRS	Systematically documenting all the requirements to figure out the what are the ambiguous parts so as to focus on them	Revisiting the requirements analysis and evaluating possible options in terms of implementation that would resolve the ambiguity
8	Wrong interpretation of SRS in Design	Proper requirement analysis, and documentation of SRS	Modification of the design plans and documents in sync with the SRS	Management and review of the work already completed based on the design plans and determining the course of action for the remaining work to be completed successfully
9	Lack of experience or training in using software tools and technologies	Learning and getting familiar with using the software tools and technologies	Working on a task in groups which have people with experience in using the software tools and technologies	Redistribution of tasks to people with better knowledge and experience of using the software tools and technologies

10	Too much complexity involved in WordPress development	Learning and getting familiar with WP's development environment	Keeping track of the project's progress and getting familiar with WordPress	Seek expertise from who are experienced developers on WordPress (eg – on WP Developers Forum)
11	Unavailability of team members	Proper planning and communication with the team members	Team members inform the team of their unavailability so that appropriate planning can be done in advance	Reallocation of the urgent and important tasks among the available team members
12	Conflicts among team members	Having healthy debates and discussions and following a defined process for coming to conclusions on the issues at hand. Working in a friendly and ethical manner.	Better communication and discussion among the team members about their thoughts and ideas regarding the task at hand	Resolving the conflict amicably to reach a conclusion with no grudges among the team members
13	Faulty work distribution	Proper planning and knowledge of team members' skill sets	Detailed discussion within the team to ensure work allotted is suits team members' skills and abilities	Reallocation of tasks based on clear understanding of team members' skills
14	Bad team management and planning by the leader	Proper planning, systematic and professional approach towards team work	Leader should discuss all his ideas, plans and policies with team members before taking decisions	Other members of the team take active part in leadership decisions

15	Entelechy website crash	Following the right development methods and standards, based on the requirements of WP platform and server	Resolve the error by executing system recovery test plans	Contact System Administrator
16	Incompatibility of two modules/plugins	Following the right development methods and standards, WP platform and server. Developing proper unit and integration test plans	Execute the unit and integration test plans to figure out the error, and resolve it.	Try to find alternative plugins or make changes in the code of the given problematic plugin.
17	DA-IICT server does not work properly	Understand the system and network requirements at client and server side before starting implementation.	Check for any version clashes of PHP, MySQL – If any, then upgrade them resolve the error.	Contact System Administrator

6. Risk Monitoring and Control

The objective of Monitoring and Control is to ensure that all steps of the Risk Management process are being followed and, as a result, risks are being mitigated and contingency plans are followed as necessary. Planned risk responses are executed as required over the life cycle of the project, but the project should also be continuously monitored for new and changing risks. Risk Monitoring and control involves the oversight and tracking of risk mitigation and contingency action plan execution, re-assessment of risks, reporting risk status, and recording risk information changes.

6.1 Risk Status

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

Analysis complete – Risk analysis is done but response planning not yet performed.
Planning complete – Response planning complete
Triggered – Risk trigger has occurred and threat has been realized.
Resolved – Realized risk has been contained.
Retired – Identified risk no longer requires active monitoring, that is, the risk trigger has passed.

S. No.	Risks	Monitoring & Control	Risk Status
1	Uncertain Product Size	Changes should be made in design structure of the product and accordingly in design documents and project plan.	Planning Complete
2	Customers/Clients do not understand the exact requirements of their organisation	Discussions with clients on requirements gathered and analysed	Resolved
3	Customer/Clients may change their requirements	Discussions and taking feedback from clients on requirements gathered and analysed	Resolved
4	Unrealistic deadlines for deliverables/milestones	No. of days to be taken as buffer before the deadlines and project timeline should be modified accordingly	Resolved
5	Not following the process defined for development	Proper monitoring of the work done and getting the work done within the std. of the process	Resolved
6	Wrong selection of the Software Development Life Cycle to complete the project in the given time and with the given team members	Management and review of the work already completed and determining the course of action for the remaining work to be completed	Retired
7	Ambiguity in requirements	Discussion with clients on requirement gathered, and taking feedback from them	Resolved
8	Wrong interpretation of SRS in Design	Review of requirement analysis and design specifications	Resolved

9	Lack of experience or training in using software tools and technologies	Work should be distributed amongst the members on the basis of the skills set and if possible learn them in due course of time	Retired
10	Too much complexity involved in WordPress development	Proper learning time should be incorporated in the planning – for members to learn and explore the platform.	Retired
11	Unavailability of team members	Work should be transferred to other members as soon as possible and proper monitoring of the project work done by every team member	Resolved
12	Conflicts among team members	Proper understanding between the team members. Team leader must ensure that a healthy work environment is created.	Retired
13	Faulty work distribution	Work should be distributed on the basis of skill sets of team members	Retired
14	Bad team management and planning by the leader	Review of the plans and proper discussion with team members on planning	Retired
15	Entelechy website crash	Build a robust website and test it exhaustively	Planning Complete
16	Incompatibility of two modules/plugins	Integrate different modules as soon as they are made rather than at the end	Resolved
17	DA-IICT server does not work properly	Test the website on institute server	Planning complete

…

7. References

Sandeep Mertia, et. al, Project Plan, Team 7, IT314 Software Engineering, Winter 2012-13, DA-IICT

Sandeep Mertia, et. al, Software Requirements Specification, Team 7, IT314 Software Engineering, Winter 2012-13, DA-IICT

IEEE Standard 1012-1998: IEEE Standard for Software Verification and Validation

Solanki, Aakash, et. al, Risk Management Plan, Team 16, IT314 Software Engineering, Winter 2011-12, DA-IICT