Risk Management
Version 1.0
Online Pharmacy

Team: CS – 01 (D-Enigma)

1) Executive Summary

Risk management is an ongoing process that continues through the life of a project. It could have either a positive or negative impact to a project. A risk may have one or more causes and, if it occurs, one or more impacts. All projects assume some element of risk, and it's through risk management we get the potential to identify those event that have an impact the outcome of a project.
Identification of risk normally starts before the project is initiated, and the number of risks increase as the project matures through the lifecycle. After a risk is identified we should find the probability of occurring, the degree of impact to the schedule, scope, cost, and quality, and then risks are prioritized. The probability of occurrence, number of categories impacted and the degree to which they impact the project will be the basis for assigning the risk priority.

1.1 Purpose

The main purpose of this document is to identify risks and control those which may have negative impact on the project. In this document we will cover all the six phases which are:

- Risk Identification
- Risk Assessment
- Risk Mitigation
- Risk Contingency Planning
- Risk Tracking and Reporting
- Risk monitoring

2) Risk Management Strategy

2.1 Risk Identification

Risk is any event which on occurring prevents the project from progressing as planned. Some risks are obvious and can be identified initially. It is good if we can identify the risks before the project and some the risks can only be identified during the project life cycle.

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. A Risk Management Log will be generated and updated as needed and will be stored electronically in the project library.

Documentation of risk must include the following things:
• Description of risk factor and probability of its occurrence.
• Schedule impact, scope impact, quality impact, cost impact.

2.2 Risk Responsibilities

Risk Management should be done by each and every of the member of the group. If the risk can be resolved at team level, the decision of group leader will be final but if the risks are major and can't be resolved by the team members, the decision will lie with the client.

2.3 Risk Response

For each risk which we identified in risk identification we need to find an appropriate response for it. It is done by every member of the project team. The best risk assessment will help us in identifying the best risk response. The probability of occurrence of risk and its impact on project cycle determines the degree of risk. The following may be the response options:

• Avoidance: The main objective is to avoid the risk by changing the scope of project.

• Mitigation: This is the most used technique and it minimizes the impact and probability of risk. It is done by taking early action, continuous monitoring etc.

• Acceptance: In this technique we accept the risk and impact caused by the risk. It is good for small risks whose probability of occurrence is low and do not have much impact on project.

• Exploit: This technique is used when risk has positive impact on the project. In this we search for ways to make the risk happen and increase its impact.

2.4 Risk Mitigation

Risk Mitigation allows a team to develop ways of minimizing the likelihood of occurrence of a risk or the damage it can do. The risks are either eliminated by eliminating their causes or measures are taken so that the causes are prevented from occurring.

2.5 Risk Contingency Planning

Risk contingency planning is sequence of action designed to help project team if the there is a potential of occurrence of the risk in the future.

2.6 Risk monitoring

Software risk monitoring is integrated into project activities and regular checks are conducted on top risks. Software risk monitoring comprises of:

- Tracking of risk plans for any major changes in actual plan, attribute, etc.
- Preparation of status reports for project management.
- Review risks and risks whose impact or likelihood has reached the lowest possible level should be closed.
- Regularly search for new risks.

3) Types of Risks

There are three main types of risks:

3.1 Project Risk

- Budgetary Risk
- Schedule Risk
- Personnel Risk
- Customer-related Risk

3.2 Technical Risk

Technical risks include problems related to maintenance, implementation, design, testing. Changing requirements, incomplete requirements are also the part of technical risk. Most of them usually occur insufficient knowledge of team about the project.

3.3 Business Risk

Building a product that no one wants. Budgetary loss and personnel commitments also come into Business risks.

4) Risks Mitigation and Monitoring

4.1 Late Delivery

Severity of risk: *Catastrophic Risk*

Type of risk: *Scheduling Risk*
Probability: 3

• Mitigation: The cost associated with late delivery is critical. Late delivery will result in entire team not getting any marks for entire project and more importantly it may result in rejection of project by the client. Steps have been taken to ensure a timely delivery by dividing the project into multiple stages and at the end of each stage we will have something deliverable.

• Monitoring: A schedule has been established to monitor project status. Falling behind schedule would indicate a potential for late delivery. Adjustment to schedule will be done if we are not matching the schedule and effort will be adjusted accordingly.

• Management: Late delivery would be a catastrophic failure in the project development. If it becomes apparent that the project will not be completed on time, the only course of action available would be to request an extension to the deadline from the professor.

4.2 Lack of Development Experience

Severity of risk: *Critical Risk*
Type of risk: *Technical Risk*
Probability: 5

• Mitigation: In order to prevent this from happening, the development team will be required to learn the languages and techniques necessary to develop this software. The member of the team who are most experienced in a particular area of the development tools/techniques will need to instruct those who are not as well versed.

• Monitoring: Each member of the team should watch and see areas where another team member may be weak. Also if one of the members is weak in a particular area it should be brought to the attention by that member, to the other members.

• Management: The members who have the most experience in a particular area will be required to help those who don't have experience in that area. It should come to the attention of the team that a particular member needs help. Members who lack experience should tell the team members about their situation. Honesty is very important in order to manage this risk.

4.3 Absence of a Team member (due to disease or some other emergency)

Severity of risk: *Catastrophic Risk*
Type of risk: *Personal Risk*
Probability: 4

- Mitigation: This is something which can't be prevented but we can minimise the damage caused by this risk.

- Monitoring: We will try to detect this risk by keeping in contact with all the team members and each & every member is comfortable taking about their problems with the group.

- Management: If this occur, the team would call a meeting. In this meeting depending upon the absence of the team member we will redistribute the work among the other group members to cover up for absence. And we may also need to reschedule deadlines. Also we will discuss how the member can cover up for his/her absence.

4.4 Poor Quality Documentation

Severity of risk: *Critical Risk*
Probability: 5

- Mitigation: Meetings will be held routinely to offer documentation suggestions and topics. Any topic missing by a particular member will be discussed and it will be decided whether or not to add that particular topic to the documentation. All the documents will go through two rounds of review, one is structure review and the other is the content review.

- Monitoring: We will observe changes made from time to time in different document and make sure that it adheres to the standard we are maintaining.

- Management: If this occur, the team would call a meeting and discuss the modification of existing topics, addition of new topics, or removal of unnecessary topics into the documentation. Also, we will consult our TA mentor in case of doubt.

4.5 Risk: Deviation from Software Engineering Standards

Severity of risk: *Critical Risk*
Type of risk: *Technical Risk*
Probability: 4

• Mitigation: While it is possible to deviate from software engineering standards, it is unlikely to occur. All team members have an understanding of the software process and we plan to implement them in the process.

• Monitoring: Technical reviews involving comparison between documentation and the actual project will help to determine if deviation will occur. All relevant documents must be as complete and as accurate as possible to ensure that work will conform to expressed software engineering standards.

• Management: If deviation occur, steps must be taken to guide the project back within the standards expressed in accompanying documents. Technical reviews help to determine what must be done to keep the project in line with established software engineering standards.

4.6 Organizational inefficiency

Severity of risk: *Critical Risk*
Type of risk: *Personal Risk*
Probability: 4

• Mitigation: Tasks among the team members should divided upon their capabilities and the workload should be divided as much equally as possible.

• Monitoring: Active participation of all the team members is required and continuous suggestions should be given by all team members to the team leader which reduces the organizational inefficiency.

• Management: All the team members should complete their work before the deadlines and act according to the team plan and regular discussions with team members are helpful.

4.7 Conflict between Team Members

Severity of risk: *Catastrophic Risk*
Type of risk: *Personnel Risk*
Probability: 5

• Mitigation: Each and every member of the team is responsible for anything that happen in the project. The workload should be divided as much equally as possible. Maintain mutual understanding between the members. Honesty among team members is very important.

• Monitoring: Have clear understanding of goals that are to be achieved. While reviewing no one should do anything based on personal grudges. Work must be distributed according to the capacity of each person.

• Management: Discuss all the issues, with the team whether they are small or large. Don't blame each other. If problem is not solved within the team then consult project mentor or professor.

4.8 Not Meeting Deadline

Severity of risk: *Critical Risk*
Type of risk: *Scheduling Risk*
Probability: 6

• Mitigation: Manage the work properly such that delay should be minimum. Constantly review the work done to check the lag time.

• Monitoring: Have clear idea of the dates and deadlines of each phase and milestones of each phase. Check whether the assigned work is completed in time or not.

• Management: If work load is more on some sub group, members of other sub group must coordinate with them in order to complete the assigned work within given time. If the deadlines haven't been met, do rescheduling accordingly (if required).

4.9 Inability of technology to provide a particular feature

Severity of risk: *Catastrophic Risk*
Type of risk: *Technical Risk*
Probability: 4

• Mitigation: Technology should be chosen such that it satisfies all the requirements.

• Monitoring: The team will stay regularly updated with the technology. They will

• Management: If the technology is unable to provide a feature, the requirement of feature will be discussed with the client and if it is must, then accordingly the technology will be changed or adjustment will be made (if possible).

4.10 Test cases not covering everything

Severity of risk: *Catastrophic Risk*
Type of risk: *Technical Risk*
Probability: 5

• Mitigation: Make test cases in such a way that they should cover all the requirements specified in the SRS and all the queries in the database should also be covered.

• Monitoring: After the test cases are created they should be reviewed multiple times and find out and add all the missing and required test cases.

• Management: While preparing test case make sure that all the aspects of project are covered in test cases. If any test case is missing, all the team members should discuss and then should decide what to do. If it is not solved among team members consult mentor or professor.

4.11 User experience not being good

Severity of risk: *Catastrophic Risk*
Type of risk: *Customer-Related Risk*
Probability: 6

• Mitigation: Make the user interface such that it's easy to learn and users feel comfortable with it. Make sure it's good looking but more importantly make sure that it is easy to navigate and work with.

• Monitoring: After the design of each screen, make sure that the design is verified in the team and then try to get it verified by a person outside the team.

• Management: If this risk appears, we will go back to the design board, study the user's usage of application and then make changes to the design accordingly.

4.12 Improper work distribution
Severity of the risk: *Catastrophic Risk*
Type of risk: *Personal Risk*
Probability: 4

- Mitigation: Distribute according the skills of the team members in mind and make sure to distribute the work equally. Make sure to set deadlines for every task with some flexibility.
- Monitoring: The team leader should make sure to check the work done by other members from time to time and should make sure that the deadlines are met.
- Management: Re-asses the strengths and weaknesses of the team members and divide the work among. If any member is interested to learn something new allot him the work and tag along a member who is good at the same task.

4.13 No Synchronization with each other's work
Severity of the risk: *Catastrophic risk*
Type of risk: *Personal risk*
Probability: 6

- Mitigation: Maintain a version control tool like Github or Bucket where you can update all the changes done in development. Another advantage of maintaining a tool like this is we can easily know who the responsible person for the change is.
- Monitoring: Every member of the team should maintain contact with other members regularly so that these kind of problems are not caused.
- Management: Call an urgent meeting with all the members and re-synchronize the work done. Also make sure that this kind of mistake is never happened again.

4.14 Too many changes in requirements
Severity of the risk: *Catastrophic risk*
Type of the risk: *Technical risk*
Probability: 4

- Mitigation: While collecting the requirements make sure all the areas are covered. If there are any changes to be done, study the requirements once again and make proper plans to incorporate changes in.
- Monitoring: Once a change is done on requirements, team should make sure that's the last change done in that phase. Changing a change regularly isn't good while developing an application.
- Management: Analyze the reason behind the change and think about whether the change is really required or not? If the whole team thinks it is required, then amend the work and make sure that the following change wil be the last in that phase.