Risk Management Report

Table of Contents

Introduction

In this document, it shall be reviewed how the various stages of risk management could have been applied to our project, had we been aware of them at the time, as well as seeing what the risks are from this point onwards. These two risk assessments have been done because our group is so far ahead with the project that it is just about finished, so we would not have much to say just by looking at the risks from this point onwards.

The relevant stages in risk management are *risk identification, risk planning* and *risk monitoring*. Of course, no retrospective assessment could be entirely accurate as risk management is a process that starts at the beginning of the project and continues throughout.

For risk identification, it shall be examined what possible risks could have occurred as well as identifying the setbacks that did occur. For risk planning, it will be seen which risks could have been and can be avoided and what contingency plans could and have been made. For risk monitoring, it shall be looked out how we have monitored the risks throughout the project and how we shall continue to do this.

Risk Identification

The risks that could occur, and indeed did have been split into a number of sections that are detailed below:

(a) **Pre-programmed components**
- i) At the beginning of the project, it was not planned for us to use any pre-programmed components so at the time we would not have said there was any risk involved with these.
- i) We have so far not used any pre-programmed components and so have encountered no problems with them.
- i) We do not plan to use any pre-programmed components in the remaining part of the project.

(a) **Personnel illness/unavailability**
- i) Before the project began it was not really anticipated that there would be any problems with group members being ill or leaving the university. The risk of this happening would probably have been said to have been low.
- i) So far, there have been minor problems due to illness during this project, but nothing that had any effect for more than a couple of days.
- i) One major problem that did occur during the project was that one member of the group left the university.
- i) There is of course the possibility of further personnel illness in the remainder of the project, but this is only thought to be of low risk, although you never can be sure.
- i) We feel there is a moderate risk of group members not doing the work they have been asked to do, especially over Easter.

(a) **Organisation risks**
- i) Due to the nature of the project, organisational risks were minimal, although we knew from an early stage to look out for things such as ‘requirements creep’ due to the experience of a group member who was retaking the year and had done the Software Hut project previously.
- i) In actual fact, there has been very little change in the client’s requirements, and it was a condition of this project that the requirements be frozen after five weeks. However, until the Week 5 cut-off point, changing requirements was certainly a possibility.
- i) When, after Easter, our system is shown to the client, we think there is a moderate chance of them wanting us to alter the system to fit in some new requirements. However, we think this presents only low risk because Professor Mike Holcombe has instructed us not to alter our system for any late requirement changes due to the lack of time.

(a) **Tool risks**
- i) The only tool risks in the project were associated with the Symantec Café tool used to generate code, particularly the graphical user interfaces. Having used this product in the past and found no reliability problems, we would have thought at the beginning of the project that there was only a low risk of the project being affected by Symantec Café not functioning properly.
- i) So far, Symantec Café has worked very well, although there have been some problems with it only working on certain computers in the Lewin Lab. However, these problems have not led to any difficulties.
- i) Having finished creating the program, we have no more need for any tools and so the estimated risk due to tools for the remainder of the project is none.

(a) **Technology risks**
- i) At the start of the project, technology risks were considered to be the biggest risk to our system not being a success.

i) The risk basically was that either the system would be too difficult to produce given the networking requirements, or it would be produced, but just not work on the clients' computer systems.
i) The members of the group have little experience in networked technologies so initially we wondered if the system could be created.
i) The main risk was not finding somewhere for the server to be located.
i) We have managed to implement the system and get it to work properly within the Department of Computer Science, but it is still unknown whether it will work on the client's machines.
i) Due to the client not cooperating, it is even unknown what exactly the facilities are that the client can provide.
i) Attempts at getting CICS or DCS to host the system have proved unsuccessful.
i) As things stand at present, we feel there is a moderate to high risk concerning whether the system will work on the client's computers or not.
i) There have also been technology problems concerning the CICS and DCS computers. At the beginning, we did not anticipate problems with the machines but there have been some times when group members have been unable to log-on. The effects of this were not serious, although we did lose a few hours.
i) We think the computers may not be working at a few points after Easter, but as we have nearly finished the project, there should be little risk involved with this.

To summarise, the main risks at the beginning of the project would probably have been identified as follows:

1. Our group not being able to create the system.
1. The system not working on the client's machines.
1. Changing requirements.

The main risks from this point onwards are:

1. The system not working on the client's machines.
1. Personnel illness/unavailability.
1. The client wanting to make changes to the system.

Risk Planning

In this project, we did not have a Risk Management strategy, and therefore no formal risk avoidance or reduction plans. The only problems that we had only resulted in a small amount of lost time, which was easily made up. The departure of one group member did not affect our plan, as at the time we had no formal plan.

Personnel illness/unavailability was compensated for by simply making up the work later. Changing requirements was an inherent part of the project, but the effects were not serious and did not need to be compensated for. If Symantec Café was unusable, we would simply have had to program the frames manually. Of the problems listed, none could be avoided; they could only be compensated for.

In terms of planning to avoid the risks that might occur in the remainder of the project, we have down the following things:

(a) **The system not working on the client's machines**

This could well lead to the program not working at all, which could in turn lead to us getting a very low mark. The risk to the project due to this was considered so high that it was decided to build a standalone version of the system.

This version should have no problems working on the client's machines because all the problems and uncertainties so far have been to do with finding somewhere for the server of the system to go. It will not have any of the monitoring facilities of the networked version, but these were only desirable requirements anyway, and not mandatory.

The task of producing the standalone system has been assigned to Andrew Cubbon, who will produce it over Easter. It is anticipated it should not be too difficult to produce, due to it mainly involving just deleting parts of the present system.

(a) **Personnel illness/unavailability**

In case of group members being ill, their work will just have to be redistributed among the remaining members. To try to make sure group members do the tasks assigned to them, it has been stated precisely what each group member has to do over Easter and strict deadlines for work submission have been set. Group members know that the marks for the project may not be distributed evenly in the case of group members not doing their fair share.

For further details of this, please see the "*Time Plan*" document for the Easter vacation.

(a) **The client wanting to make changes to the system**

The plan in case this occurs, is to say to the client that we have been instructed by Professor Mike Holcombe not to make any significant changes to the system at this late stage. If, however, the changes were minor, then we would try to make the alterations the client required.

Risk Monitoring

As has been stated, many of the risks that continue to affect the project have been anticipated from the beginning and have therefore been informally monitored. The progress on certain issues, such as finding out where the server can be put, have been reported every week at the group meetings so that all group members are aware of the current situation and the relevant action can be taken.

From this point onwards, we can now adopt a more structured monitoring approach. Over Easter, the progress of the tasks that have been set will be recorded and after Easter, each of the main three weeks shall be monitored weekly to see if the risk is reducing as it should be. The monitoring will be recorded on forms, such as the one shown on the next page.

Risk Monitoring Form

Date: / /

Author:_____

Risk summary: _____

Current risk situation:

_____
_____
_____
_____

Current risk assessment (tick the appropriate box):

- q Low
- q Low-moderate
- q Moderate
- q Moderate-high
- q High
- q Very high

Recommended action:

_____
_____
_____
_____
_____

Conclusion

To summarise, we think that although many of the risks that initially faced the system have now been resolved, some risks still exist. However, with the contingency plans (particularly the standalone system) that we have put into action, we feel that these risks can be minimised.

We feel that risk management is a useful technique and it would have been useful to have learnt more about it nearer to the beginning of the project rather than at this late stage. Still, we feel that even now it can be useful and we will try to use it to good effect in the remaining six weeks of the project.