Risk assessment and mitigation (3)

Introduction

To manage risk within our project, we decided to produce a risk register. A risk register is an effective tool to identify issues and plan mitigation techniques to avoid them. The register is also a good tool to provide documentation to the group, as to what to do in the event of an issue. Within the risk register, risks are detailed and then categorized into groups which are related, for example, bugs during coding are categorized as technology issues. Severity and likelihood levels are then assessed for each risk and mitigation techniques are tailored to avoid, limit or accept consequences. The level of detail used within the risk register is low to moderate and includes the type of mitigation used. This has been done purposefully as the risks themselves are nonspecific and can happen at anytime, to any member of the team. As such, mitigation techniques must also be nonspecific in an attempt to combat all possibilities. The risk register was systematically updated throughout each assessment to ensure we always had the most recent version available. During our scrum meetings, we mentioned any new risks that we came across and these were then added to the risk register by the documentation lead.

Types of Mitigation:

- Risk Acceptance: Does not mitigate the risk as the cost of doing so outweighs the damage of the risk
- Risk Avoidance: Mitigation designed to avoid the risk altogether
- Risk Limitation: Mitigation that, when an issue occurs, works towards reducing the damage of the issue
- Risk Transference: Mitigation that transfers the issue to a 3rd party.

Severity Levels:

Severity levels are a description of how harmful a risk may be if it were to occur. A risk can be harmful in one of two ways, either a risk degrades the quality of the project or a risk can cost time to resolve.

	Low	Medium	High
Quality	Requirements mostly met	Requirement partially met	Requirement not met
Time	A Day	A few days	A week or more

Likelihood Levels:

Low - Will almost certainly not happen
Medium - Has equal chance of happening or not happening
High - We expect this to happen at some point
Almost certain - This will almost definitely happen at least once

Risk Identification Process:

After reviewing feedback from assessment 1, we decided to included information regarding our risk identification process. Our process involved each member being allocated a risk category (i.e. tech, people, requirements, estimation) and coming up with a list of possible risks that may occur during our project along with their severity and likelihood. Then, we had a team discussion which involved going over each risk and deciding on a mitigation. This was useful as everyone got a say and collectively generated more ideas (different methods of mitigation). We decided to use three severity levels and four likelihood levels to help simplify the process.

Risk matrix:

A Risk matrix was produced to provide an overall risk as the product of the likelihood levels and severity levels. This is a simple mechanism to increase visibility of risks and assist decision making. The higher the overall risk of an issue (higher number), the more dangerous the issue is to the project, as such more planning will go into attempting to mitigate or avoid issues with higher overall risk. On the other hand, issues with less overall risk represent issues that may be ignored, as they may not be too damaging or are very unlikely.

		Severity Levels		
		Low	Medium	High
Likelihood levels	Low	1	2	3
	Medium	2	4	6
	High	3	6	9
	Almost Certain	4	8	12

Risk Register

*Overall Risk is calculated from risk matrix

ID	Category	Description of Risk	Severity	Likelihood	Overall Risk*	Mitigation	Risk Ownership
1	Tech	Data Loss due to unforeseen circumstance	High	Low	3	Avoidance: Utilisation of 3rd party services to store online backups	Technical lead
2	Tech	Bug in development environment	Medium	Low	2	Avoidance: All tools the team uses are well tested.	Technical lead
3	Tech	Incompatible software update to 3rd party software	High	Low	3	Acceptance: All affected code and software must be updated	Technical lead
4	Tech	Hardware compatibility issues	High	Low	3	Acceptance: Software stability suffers	Technical lead
5	Tech	Game lacks stability and crashes	Medium	Medium	4	Limitation: Software tested on final platform as coded, stability issues will be fixed as they are found	Technical lead
6	Tech	Unity not working on lab PCs	Medium	Almost Certain	6	Acceptance: Each team member installs unity on their laptop as a back-up	Technical lead
7	Tech	Code changes breaking existing code	Low	High	3	Avoidance: Use existing tests to ensure we are not changing existing behaviour	Technical Lead
8	People	Arguments within team	Medium	Medium	4	Limitation: Speak to Lecturer to act as a moderator	Project Manager
9	People	Team member is unavailable	Medium	Almost Certain	8	Limitation: member's work is split between remaining members depending on who has the least work	Project Manager

10	People	Team member is lacking critical knowledge	Medium	Almost Certain	6	Limitation: Basic training on new languages or tools	Project Manager
11	People	Miscommunication	Medium	Almost Certain	8	Avoidance: Some documents are created for the sole purpose of aiding communication between members, e.g Gantt chart	Project Manager
12	People	Under-communication	Medium	High	6	Avoidance: The team holds 2 face to face meetings per week in addition to semi-regular online communication.	Project Manager
13	People	Uneven workload	Medium	Medium	4	Avoidance: Team members with little work are encouraged to participate in or review other parts of the project.	Project Manager
14	People	Total loss of team member	High	Low	3	Acceptance: Talk to lecturer to discuss methods to proceed with more assistance	Project Manager
15	Requirements	Misunderstanding requirements	Medium	High	6	Limitation: All work is peer reviewed and obvious issues are resolved before they are used for other elements of the project	Customer Interface
16	Requirements	Requirements change	High	Almost Certain	12	Limitation: Team uses the scrum methodology, to more easily accommodate changes to the requirements.	Customer Interface
17	Requirements	Architecture doesn’t work / unfit for purpose	Medium	Medium	4	Avoidance: sequence diagrams were created to run through the architecture to reason its workings.	Customer Interface
18	Requirements	Conflict between different stakeholders	Medium	Medium	4	Limitation: The team would act as a moderator between the two stakeholders, and attempt to resolve the issue into a compromised requirement	Customer Interface
19	Requirements	Ambiguous requirements	Medium	Medium	4	Avoidance: All requirements were peer reviewed to avoid ambiguity.	Customer Interface
20	Requirements	Inflated Requirements	Medium	High	6	Avoidance: During the listing of our requirements,	Customer Interface

						each requirement was labeled with a priority, which indicates how vital it is to the project. Almost all optional requirements were removed	
21	Requirements	Stakeholders have inaccurate expectations	Medium	Medium	4	Avoidance: Meetings were held with stakeholders to clear up ambiguous issues within the requirements	Customer Interface
22	Requirements	Requirement differences between our group and the group whose project we picked up	Low	High	3	Acceptance: Before starting implementation, discuss requirements as a team and select which requirements to adopt as part of the change management procedure.	Project Manager
23	Estimation	Unexpected program complexity	Medium	Medium	4	Acceptance: More time is issued to the problem to allow its completion	Secretary
24	Estimation	Incorrect severity and likelihood assessment in risk register	Medium	Medium	4	Avoidance: Multiple team members check our risk analysis to avoid obvious mistakes	Secretary
25	Estimation	Overly optimistic schedule	Medium	Medium	4	Limitation: When required, schedule more time for problematic tasks.	Secretary
26	Estimation	Team members losing time trying to understand the code and architecture of the product from the other team	Medium	Medium	3	Avoidance: We do not have to understand all of the code to make changes, only need to understand the interface you are changing/adding to.	Secretary