Risk Management

Our risk management process involved 4 steps - Identification, analysis, planning and monitoring.

The first step, identification, involved us discussing as a team the possible risks associated with the project. We identified whether the risks were to the project, the product or both, or business, in order to categorise them in a more logical way. Additionally, when considering the risks, we focused on different areas of the project in order to assist the discussion. This included areas such as People and Technology.

The second step, analysis, required us to reflect on the potential risks we generated in the first step and judge the likelihood and severity of each of them. We also removed any risks which we deemed of very low probability or severity. We judged the risks on a simple scale of 1-5, with 1 being low likelihood/severity and 5 being high likelihood/severity. This helped us sort the risks and decide how best to address them.

The third step, planning, involved coming up with mitigation/minimisation and avoidance strategies in order to reduce the chance that the specified risk will impact the project. Our strategies included regular, clear communication, storing important files in multiple places, or online and having more than one member of the team assigned to key tasks.

The fourth and final step, monitoring ,assigning risks to team members, required the team to regularly reassess the likelihood and severity of the risks, and reporting to the rest of the team any changes that have been made. This is an important step as it ensures that each member of the team is keeping in mind the risks and steps they need to take.

The format of our register below is a 7-column table, with columns for risk ID, risk type, risk description, likelihood of occurrence, severity of the risk, mitigation strategy and the risk's ownership. The format of our table helped lay out the risks in a logical, easy to follow way, which helped us to quickly find risks of a certain type in the risk register should we need to update them or remind ourselves of the mitigation strategy.

ID	Risk Type	Description	Likelihood	Severity	Strategy	Ownership
R1	Project	A team member falls ill and cannot work on the project	3	4	● Divide work effectively between other team members	Thomas
R2	Project	One or more team members' computers breaks and they cannot work on the project	2	4	● Use university lab PCs, divide work in the meantime	Seb
R3	Project	Version control system stops working/goes down and we cannot access the project	1	5	● Keep backups of the project files, discuss other ways of collaborating	Josh
R4	Product	Code doesn't work/doesn't run/isn't optimised on demo machines	2	4	● Ensure it runs on a variety of types of machine before deployment, to increase likelihood of successful deployment	Tikhon
R5	Project	Someone loses important files	2	5	● Keep backups on multiple machines and in the cloud if	Josh

					possible	
R6	Product	Game crashes during live presentation	3	5	● Good testing and analysis during development to help reduce risk of crashes	Tikhon
R7	Product	libGDX licence changes during development	1	3	● Ensure final product adheres to licence	Seb
R8	Product and project	Customer's requirements change	2	3	● Meet regularly with client to discuss any changes. ● Adapt product to new requirements ● Use of agile methods in software engineering	Thomas
R9	Project	Communication breakdown	3	4	● Establish clear channels of communication ● Encourage open and honest communication ● Resolve conflicts as they arise.	Seif

R10	Project	Team member leaving the team	1	3	• Divide his work among team members	Seif
R11	Product	IDE crashes	1	3	• Keep backups on different IDES • Switch to another IDE	Harry