ENG1 - Assessment 1

Risk Assessment and Mitigation

Risk1.pdf

Group 6

Freya Goodger	sg1967
Mikolaj Wyrzykowski	mw2179
Barnaby Matthews	bm1287
Cooper Love	cl2702
Oliver Cassey	oc854
Anna Hrynyshyn	ah2886
Oliver Thompson	ot699

Risk Management Process

The risk management process followed by our team contains multiple steps. Every week during meetings, we will dedicate time to identifying and discussing risks. Risks will be recorded in the risk register and analysed to be designated a likelihood and a severity, which will be low, medium, or high. Severity in this context refers to the impact on the project due to the lower risk nature of the project as a whole. After this, mitigation measures can be decided. When risks are identified they will be designated at least two owners, who will be responsible for monitoring that risk. At least two owners should be assigned to each risk as this will reduce the bus factor in the requirement monitoring process. The risk should be monitored at least weekly. When a risk is monitored the owner should check whether the likelihood and severity are still accurate. They should assess whether a risk needs greater mitigation, and if so they should bring it to the attention of the group in a meeting. There will be a field in the risk register to assist with tracking this. Every time the risk is assessed the field should be updated to the current date to mark it as monitored. It is the responsibility of the owners of risk R1 to ensure risks are not being neglected and to contact the risk owners otherwise. The risk will be categorised with a type of that risk. The type can vary between the following options [1]:

- Estimation risks arise from the estimates of the resources required.
- Organisational arise from the organisational environment.
- People risks are associated with people in the team.
- Requirements risks arise from changes to requirements and managing them.
- Technology risks arise from the software or other technologies in the system.
- Tools risks come from the software tools and other software used to develop the system.

Format of Risk Register

The risk register consists of seven columns. ID contains the IDs used to refer to the risks, in the format R{X} to improve clarity if referencing the risk. Type contains the type of the risk, which can be multiple categories as discussed in the risk management process plan.
A risk can be of multiple types. Mitigation contains the mitigation and response the team will use to deal with the risk. Owners are the people who are responsible for ensuring the risk is adequately managed. Likelihood is the chance of the risk becoming an issue. Severity is the impact if the risk does become an issue. Likelihood and severity are both graded on three levels: low (L), coloured in green; medium (M), coloured in orange; and high (H), coloured in red. This system will allow for easier identification of important risks. Last assessed contains the date the risk was last assessed, which is to help ensure a risk is not neglected and allowed to become more likely or severe due to this. The format is a date in the form YYYY-MM-DD.

Risk Register

ID	Type	Description	Mitigation	Owners	Likelihood	Severity	Last Assessed
R1	Organisational	A risk is not assessed by its owner for too long of a time.	The owners of this risk should remind the owners of any risk that has fallen behind in assessment.	Cooper Anna	L	M	2024-03-19
R2	Estimation People	A team member is unable to complete a task in time.	Have at least two people working on a task, so they can take over and complete the task.	Cooper Anna Oliver Freya Barnaby Mikolaj Oliver	L	H	2024-03-19
R3	Estimation	A task is falling behind schedule due to being under-resourced.	Be prepared to reassign time and team members to tasks if it is found that they need more than expected.	Cooper Anna Oliver Freya Barnaby Mikolaj Oliver	M	M	2024-03-19
R4	Technology	An issue with GitHub or Google Workspace occurs which impacts the access to our work.	Ensure we have backups. Local copies of the Google drive and git repository.	Cooper Anna	L	H	2024-03-19
R5	Organisational Requirements	Objectives of the project weren't well-defined.	Cross-reference our plans with the brief and ensure they are not failing to meet or exceed the brief.	Cooper Anna	M	M	2024-03-19

R6	People Requirements	Miscommunication between stakeholders and the project team.	Ensure any doubts are settled between stakeholder and team, ask questions when needed.	Cooper Anna	L	L	2024-03-19
R7	Organisational Requirements	Stakeholder becomes unavailable to contact.	Ensure all queries are settled as soon as possible in case of this happening.	Cooper Anna	L	M	2024-03-19
R8	Organisational Tools	Our work is stolen or plagiarised.	Keep documents and repositories private until after submission.	Cooper Anna	L	H	2024-03-19
R9	Requirements	The game does not meet the requirements for locations to interact with in the world, i.e. study and recreational locations.	Ensure adequate time and resources are given to reach requirements in the implementation stage.	Cooper Anna	M	H	2024-03-19
R10	Organisational Requirements	The product has undergone numerous changes in its scope.	Ensure that the product and deliverables are regularly reviewed.	Cooper Anna Oliver Freya Barnaby Mikolaj Oliver	M	M	2024-03-19
R11	Technology Tools	There is a bug or other issue with the libraries we are using.	Have multiple options to fall back onto in case of a failure. Plan on how to adapt to the issue and work around it.	Cooper Anna Oliver T.	L	H	2024-03-19

R12	Organisational	Work exceeds the page limit for a specific task.	Before submission, check the assessment document and verify with our work.	Cooper Anna	L	M	2024-03-19

References

[1] I. Sommerville, “Risk management” in *Software Engineering.* Harlow: Pearson, 2016, pp. 644-651.