Risk Assessment and Management Plan (RMP)

Table of Contents

1. Introduction

The risk assessment and management plan: documents that lists hazards and risks that could affect a software project, along with mitigation or avoidance techniques. The plan's objective is to guarantee that the project is finished on schedule, on budget, and with the appropriate standard.

2. Advantages of the risk assessment and management plan

- Early identification of any possible problems allows for the necessary mitigation through suitable action.
- Risks are prioritized according to their likelihood and probable consequences, which helps the team concentrate on the most crucial problems.
- Improve project performance by lowering the risk of overruns in budgets and delays.

3. How Risks and Assessment identified among our team

Through discussion sessions where team members shared their knowledge and experiences and explored potential risks, the project team determined the risks connected with the project. The group also carried out analysis to determine the most common hazards on internet platforms and the kinds of vulnerabilities to which the project was most at risk.

The team evaluated and ranked the hazards according to their likelihood and possible consequences. The group produced a risk management strategy that comprised tactics to reduce or remove the risks that were identified as well as a method for tracking the effectiveness of the risk management measures through reporting and monitoring. The team was able to concentrate on the most significant risks and raise the likelihood that the project would succeed thanks to this thorough approach.

4. Tables

4.1. Risk management chart

Impact / Probability	Low	Medium	High
Low	R07		R02, R04, R05, R08
Medium		R06	R01, R03
High			

Figure [4.1]: Risk management chart

4.2. List of identified risks

Risk ID	Risk Type and Description	Risk Score	Resolved in Sprint	Strategy and Effectiveness
US-1.1	• Technical • Management • External • Budget • Schedule • Etc.	• Medium • High		• Mitigate • Accept • Avoid • Transfer
R01	**Time Risk:** The project is limited by the capstone timeframe, meaning once the timeframe ends, the contract with the client also ends and the project should be completed.	Impact: High Probability: Medium Risk Score: High	Sprint 5	**Strategy:** By efficient planning, we can make sure all the features we need are complete. **Strategy type:** Mitigate **Contingency plan:** Removing the more unnecessary features and saving them for last.

				When to invoke the contingency plan: Invoke the plan when the team is deviating too much off schedule.
R02	**Application Risk:** there exists the risk that our project doesn't solve the problem we intended.	Impact: High Probability: Low Risk Score: Medium	Sprint 5	**Strategy:** Survey our solution to see if it theoretically makes sense. Proper testing before more costly implementations. **Strategy type:** Mitigate **Contingency plan:** do it again next semester or replan the solution. **When to invoke the contingency plan:** when the app fails or when user testing is very negative.
R03	**Skill Risk:** there is a chance the team won't have the skill set in order to complete the project in the time frame or at all.	Impact: High Probability: Medium Risk Score: Medium	Sprint 5	**Strategy:** Proper planning and use of our programmers' skills. **Strategy type:** Mitigate **Contingency plan:** hire additional more skilled individuals to make up for the lack and teach. **When to invoke the contingency plan:** when straying too far off the schedule.
R04	**Legal risk:** The risk that the execution of the project might violate a legal convention or rule.	Impact: High Probability: Low Risk Score: Medium	Sprint 5	**Strategy**: Reviewing legal conventions or precedent is beyond the scope of our project, but making a minor change

				Strategy type: Transfer **Contingency plan:** We will revert to the old state of the system if something serious arises **When to invoke the contingency plan:** If our project leads to a serious legal problem, but this is extremely unlikely in our opinion.
R05	**Fraud risk:** The risk that our project will be exploited by one of the team members with malicious intent, for example, to steal user data.	Impact: High Probability: Low Risk Score: Medium	Sprint 5	**Strategy:** We believe that the likelihood that any of our team would do something like that is extremely low since there is almost no incentive to steal our clients' information, since it has little utility outside of the system and the legal repercussions would far outweigh the upside. **Strategy type:** Mitigate **Contingency plan:** We will forward the pertinent information to law enforcement if we believe a crime was committed. **When to invoke the contingency plan:** If we believe a malicious action has been committed.
R06	**Scalability Risk:** The website may not perform well if the number of users or operations is high due to imperfect infrastructure	Impact: Medium Probability: Medium Risk score: Medium	Sprint 5	**Strategy:** Mitigate by using a scalable and reliable infrastructure and use load testing for the platform to ensure that its scalability is acceptable **Strategy type:** Mitigate

				Contingency plan: Try alternate deployment methods and services and change the faulty algorithms if applicable **When to invoke contingency plan:**When we are severely limited by our application's performance
R07	**Team dynamics risk:** Some team members might have difficulty working together due to personal conflicts and different working styles	Impact: Low Probability: Low Risk score: Low	Sprint 5	**Strategy:** Proper team meetings and encourage team communication. **Strategy type:** Mitigate **Contingency plan:** Assess the teams composition and explore the possibility to invoke sub teams to avoid any more conflicts within team members. **When to invoke contingency plan:** When the conflict of team members persists despite initial attempts to resolve it.
R08	**Security risk:** There is a risk that our application might be vulnerable to cyberattacks, especially since none of our team members are cybersecurity experts.	Impact: High Probability: Low Risk score: Medium	Sprint 5	**Strategy:** Avoid by implementing security measures like 2FA, encryption and DDOS protection **Contingency plan:** Make a subteam that will be in charge of cybersecurity if it becomes a relevant problem **When to invoke contingency plan:** If cybersecurity threats become a credible threat to our product

Figure [4.2]: List of identified risks