**Risk Assessment and Management Plan (RMP)**

**1. Introduction**

Risk Assessment and Management Plan serves to understand and identify potential risks that may pose a nuisance over the course of our project. Uncovering the numerous types of risks, their likelihood as well as the magnitude of its severity are all a part of the risk Assessment procedure. Further managing the identified risks consists of either mitigating, avoiding, accepting, or entirely transferring the risk elsewhere. All in all, RMP will help in understanding the potential risks that can disturb the project sequence, which can allow us further to mitigate its shortcomings as much as possible.

Risks and assessments were identified as a team based on the user stories every member was assigned to. With every user story, we analyzed its implication and how potential drawbacks can lead to unwarranted risks. If a risk was identified for a particular user story, an according mitigation strategy would then be thought of to ensure that any drawbacks are minimized.

**2. Understanding used Metrics**

It is vital to understand how we define a risk and how we quantify it. For instance, we define risk as the likelihood of an event occurring that may have a severe impact on the team’s manpower. By this, we mean that anything that may pose as a nuisance to the entirety of the team is considered a risk. Given that manpower can be disrupted in several ways, we have identified and categorized types of risks below:

* **Technical**: risk that disrupts manpower regarding technology, performance, security.
* **Organizational**: risk that disrupts manpower regarding resources, dependencies, budget, management, schedule, and communication

Upon understanding the type of risk we deal with, analyzing the risk is the next step. For this, there are two metrics to consider: probability and impact.

* **Probability**: the likelihood of the risk to occur. It is important to understand that quantifying the likelihood of a risk is challenging as it involves a certain degree of certainty. To overcome this issue, we have decided to refer to our past experiences in software development within both the professional fields and team academic projects. As a team, we identified past patterns that can help estimate the likelihood of similar events occurring throughout the course of this project. We have noticed that from the identified risks in our past experiences; a risk was not close to occur or never occurred, a risk occurred at times, or a risk commonly occurred. Based on this idea, we scaled the probability of a risk to occur in 3 levels of rating: low, medium and high.
* **Impact**: The severity of the risk. Although we noticed that the severity of the impact of a risk can differ, we also noticed how the impact of a risk can be affected in various ways. For this reason, we have disclosed that an impact of a risk can be affected in 3 ways:
  + Performance: technical, personal experience, documentation
  + Schedule: delays, task dependencies, inadequate times estimates for tasks\
  + Cost: respecting budget

In addition to this, we scaled the level of impact a risk has based on the ratings below:

* + Low: has no effect on the user, can be reversed quickly, is part of the process (e.g. redesigning)
  + Medium: needs reworking, leads to poor app performance (e.g. slow loading times)
  + High: Blocks other user stories/tasks, needs a lot of reworking, leads to data loss, leads to security breach.

The probability and the impact of a risk can be identified through the usage of a risk matrix as we have done so in Section 4.

**3. Risk Assessment and Management Plan**

Given that we have identified 2 types of risks that can affect manpower, our focus on risk assessment and mitigation will be put on those as follows.

Regarding technical risks, problems such as compatibility issues, scalability challenges and data breaches are all possible. Acknowledging these risks as well as being able to mitigate them is vital in RMP. For instance, to overcome such technical risks once apparent, regular maintenance and updates to the application will address vulnerabilities and improve performance. In addition, implementing security measures such as encryption, firewalls and access controls will help protect against unwarranted access. Thorough testing throughout will also help in mitigating technical risks before deployment.

Regarding organizational risks, it’s important to recognize and consider issues such as key personnel dependency and competing priorities. To mitigate organizational risks, establishing clear channels of communication, fostering engagement amongst all team members, diversification of dependencies and resource planning are all crucial mitigations to ensure alignment with the project objectives and minimization of organizational risks.

As such, depending on the type of risk, be it technical or organizational, according mitigation plans are set in place to ensure that risks are well considered for resolvment.

**4. Risk Matrix**

The categorization of user stories can be represented in figure 1:

|  |  |  |  |
| --- | --- | --- | --- |
| Impact  Probability | Low | Medium | High |
| Low | CN-25 | CN-37, CN-32, CN-57, CN-56, CN-55 | CN-2, CN-15, CN-31, CN-66, CN-65, CN-67 |
| Medium |  | CN-29, CN-53 | CN-97 |
| High |  |  |  |

Figure 1: Risk management chart

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Risk Type and Description | Risk Score | Resolved in Sprint | Strategy and Effectiveness |
| CN-2 | Technical: Inadequate security measures can lead to data leaks | * Probability: Low * Impact: High * Overall: Medium | 1 | Avoid: Incorporate secure measures against security threats (HTTPS, input validation) |
| CN-15 | Technical: Nnprotected routes in backend can lead unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 1 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-37 | Technical: Inefficient handling of storage of profile pictures can lead to performance issues | * Probability: Low * Impact: Medium * Overall: Low | 1 | Mitigate: Implement optimized storage solutions for profile pictures |
| CN-29 | Organizational (Schedule): Ambiguous activity diagrams may result in delays due to workflow misunderstanding | * Probability:Medium * Impact: Medium * Overall: Medium | 1 | Mitigate: Collaborate with all team members to ensure everyone agrees on a consistent design that fits the overall requirements |
| CN-25 | Organizational (Schedule): Poorly designed component diagrams can lead to delays due to  misunderstanding the system architecture | * Probability: Low * Impact: Low * Overall: Low | 1 | Accept: Later design choices related to component diagrams will result in minimal cons as component driven features can always be updated internally. |
| CN-32 | Organizational (Management): Unclear vision in product statement can lead to misalignment among team members | * Probability: Low * Impact: Medium * Overall: Low | 1 | Avoid: Given that a baseline already exists in terms of the product vision, misinterpretations can easily be avoided through communication effectively as a team |
| CN-31 | Technical: Inadequate security measures could allow a user to falsely modify another user’s profile info. | * Probability: Low * Impact: Hight * Overall: Medium | 2 | Avoid: Ensure that only logged in users with valid token can modify their own profile |
| CN-53 | Technical: If a manager has many properties to manage, inadequate displaying of the properties may lead to incorrect managing | * Probability: Medium * Impact: Medium * Overall: Medium | 2 | Avoid: User a general Data Table component that can handle a lot of information and many actions. |
| CN-67 | Technical: Unprotected routes in backend can lead to unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 2 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-55 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-56 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-57 | Design: In-adherence to the design could lead to submitting incorrect information to the form and corrupt the database. | * Probability: Low * Impact: Medium * Overall: low | 2 | Avoid: Adhere to the UX designs and follow the class diagram to ensure all the necessary data are passed. |
| CN-65 | Organizational (Schedule): Due to the complexity of the user story, it is a blocker for other user stories (CN-66 and CN-67). Delays in this user story delay the entire project | * Probability: High * Impact: High * Overall: High | 2 | Mitigation: divide the story down into smaller tasks that can be done simultaneously and divide them among members to ensure faster development |
| CN-66 | Technical: Unprotected routes in backend can lead to unauthorized access | * Probability: Low * Impact: High * Overall: Medium | 2 | Avoid: Implement route protection mechanisms and regularly review its configurations |
| CN-97 | Organizational (Schedule): Since this is the first main user story for the mobile app, delays in would leave to delays in subsequent stories. | * Probability: Medium * Impact: High * Overall: High | 2 | Mitigate: Divide the user story on multiple subtasks that could lead to smoother development. |