CraftVerify

Project Plan

Team Natural Selection

Team Members:
Kameron Ferrer
Aiden Hocks
Jacob Phillips
Parth Thanki
An Nguyen
Khuong Nguyen

GitHub Link:

https://github.com/Natural-Selection491/CraftVerify

Date: 1/17/2023

Version	Editors	Updates	Dates
1.0	An, Khuong	Implement changes in Risk Management and Project Roadmap	01/08/2023
1.1	Khuong	Add Additional Risks	1/10/2024
1.2	Khuong	Add Risk Mitigation Plans	1/12/2024

Table of Contents

Project Risks Analysis and Management

Purpose

- The primary purpose of risk analysis and management is to promote a fast-paced working environment by analyzing all of the possible risks that may interfere with our project roadmap and creating backup plans to minimize their impacts.

Risk Analysis

- We will split and organize all of the risks that apply to our team members and project into three levels of threat and probability: High, Medium, and Low.

Threat Level

1. High: A high threat level indicates the risk poses a severe threat to stop the product progress and the due dates when we do not follow the mitigation plan, address the risk, and follow the management plan for when it already happens.
2. Medium: A medium threat level indicates the risk poses a medium threat to impede the product progress that results in pushing the due dates when we do not follow the mitigation plan, address the risk, and follow the management plan for when it already happens.
3. Low: A low threat level indicates the risk poses a minimal threat to the product progress that is prevented by the mitigation plan or managing the risk with the management plan.

Threat Probability Level

1. High: Risk with threat probability ranging from: 69.99% < x <= 100% are considered risk with High Threat Probability.
2. Medium: Risk with threat probability ranging from: 29.99% < x <= 69.99% are considered risk with Medium Threat Probability.
3. Low: Risk with threat probability ranging from 0% <= x <= 29.99% are considered risk with Low Threat Probability.

Possible Risk

1. Unplaned Sick or Absence Team Members
    a. Threat Level: High
    b. Threat Probability Level: High
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We need everyone to report the date, time, and reasons for being sick or absent as soon as possible(to prevent infection from spreading in case of a highly susceptible virus).
    e. Management Plan:
        i. The presented members need to hold a meeting as soon as possible and devise a plan to split the assignments of the missing member, change the order of the assignment priorities(if possible), reassign the internal due dates, or negotiate with the project manager on the external due dates.

2. Failure of Time Management(for Research Time, Designing Time, Coding Time, Testings Time, Deployment Time, etc.)
    a. Threat Level: High
    b. Threat Probability Level: High
    c. Tolerance Hours: 5 - 8 Hours
    d. Mitigation Plan:
        i. We will use the burnt-down charge and the sprint stand-ups to keep track of each member's progress to prevent the buildups of wasted time.
    e. Management Plan:
        i. If a team member cannot manage their time, the whole group will need to meet as soon as possible, create a detailed plan, and assign another team member to help and complete the assignment on the assigned external due date. We will also need to analyze the problem and determine if further action needs to be taken, such as moving the internal deadline or negotiating with the project manager on possible solutions.

3. Changes in User Roles and/or Functional Requirements
    a. Threat Level: High
    b. Threat Probability Level: High
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We will need to check and adhere to the coding standards for features and core components to have some abstraction padding to prevent the need to hardcode the changes.

    e. Management Plan:
        i. When we need to change the User Roles and/or Functional Requirements, the abstraction padding will allow us to change or replace the necessary components. We will also need to schedule a meeting as soon as possible to recalculate the time and change the internal due date to fit the required changes.

4. Technology Stack Failure
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We will only use the provided technology stacks or the technologies the professor approved through the DAR reports to prevent unwanted complications.
    e. Management Plan:
        i. When the given or approved technology stack fails, we will try to find the error and fix it as soon as possible, and we will have to find a different technology option and get it approved through the DAR report to use it for our project.

5. Hardware Failure
    a. Threat Level: High
    b. Threat Probability Level: High
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We will try to keep our hardware equipment security and version up to date and safe from hacks, bugs, and viruses to keep the hardware from being compromised.
    e. Management Plan:
        i. We will identify the failures as soon as possible, find fixes, find possible replacements in case of irrecoverable failure, and recalculate the progress to determine whether we will need to change the internal due date and/or negotiate with the project manager for other possible fixes.

6. Losing Team Member
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. There is not much we can do to prevent team members from

leaving or dropping the class, but we will try our best to help any team member who falls behind in work as long as they have a valid reason and a determination to stay. We will also need to ask everyone to notify the group if they decide to drop or leave the class(or group).

e. Management Plan:
    i. When a team member decides to drop out, we need to hold a meeting and devise a different working schedule to keep up with the internal due dates as soon as possible. We also need to notify the project manager and ask for immediate action.

7. Dependency Failure
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. To avoid dependency failure, we will make sure that we prioritize assignments from most important to least important and split the work based on the order.
    e. Management Plan:
        i. We will help each other finish the needed libraries and assignments as fast as possible to resolve the problem as fast as possible, preventing the backup work, and continue to work on the assigned work after the problem is solved. The abstraction padding within our design and coding standard will help with this problem.

8. Parth Leaving 1 Month For Business Reason
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: 10 - 14 Hours
    d. Mitigation Plan:
        i. Irremediable Risk.
    e. Management Plan:
        i. Parth will be available to work on the project during the leave and he will participate in some online meeting through Discord.

9. Late Deliverables
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: 10 - 12 Hours

d. Mitigation Plan:
    i. Our team will follow the designed project plan and regular sprint standups to check everyone's progress closely to prevent anyone from falling behind, and we will regularly check the project plan and keep everyone up to date with the project progress, work items, and milestone due dates.
e. Management Plan:
    i. When we deliver assignments and work items late, we will change our internal deadlines and create a plan to ensure everything is complete before the final testing and submission.

10. Changes In Client Deadlines
    a. Threat Level: High
    b. Threat Probability Level: Low
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We will follow the project plan, check for possible changes in the due dates, and inform everyone within the group before the changes cause other problems.
    e. Management Plan:
        i. Depending on the deadline changes, our team will hold a meeting as soon as possible to address the changes in the deadlines and create a plan to make sure the work items and assignments are completed and tested by the time of the new dates.

11. Requirement Creeps
    a. Threat Level: High
    b. Threat Probability Level: Medium
    c. Tolerance Hours: >= 4 Hours
    d. Mitigation Plan:
        i. Our group needs to hold meetings regularly to check individual team members and the project's overall progress to prevent unwanted and unnoticeable leftover work items and assignments.
    e. Management Plan:
        i. In case of requirements creep happening, we will need to create a plan to address the problem and find a way to solve it, or we will need to schedule a negotiation meeting with the project manager.

12. Going Over Budget
    a. Threat Level: High

b. Threat Probability Level: Low
c. Tolerance Hours: 10 - 12 Hours
d. Mitigation Plan:
    i. We will only use free software within the tech stack and the software that passes the DAR reports.
e. Management Plan:
    i. There are two approaches to solving this problem. The first approach is for us to find a free alternative and submit a detailed DAR report to get the new software and replace it with the old software. The second approach is to use the approved paid software and split the cost equally among the team members.

13. Gaining Team Members
    a. Threat Level: High
    b. Threat Probability Level: Low
    c. Tolerance Hours: 10 - 12 Hours
    d. Mitigation Plan:
        i. We have to hold a team meeting to check whether we want to accept a new member if we are allowed to choose between acceptance and rejection.
    e. Management Plan:
        i. Our team has extra features and functionality for phase 2, so we can add some of those features into the project for the new team member and negotiate with the project manager.

Resources

Team Capacity

Team Member	**Kameron**	**Aiden**	**Parth**	**Jacob**	**An**	**Khuong**
Weekly Capacity (Hours)	**12**	**12**	**12**	**12**	**12**	**12**
Total Weekly Capacity (Hours)	**72**					

Roles

- Project Manager
    - The project manager needs to track and test each functionality to meet the promised standards and requirements. In addition, the project manager also needs to track the team's process to ensure everyone meets each milestone's requirements.

- Team Leader
    - The team leader needs to keep everyone working on track to meet application requirements.

- SCRUM Master
    - Make sure that everyone is focusing on their work and following the sprint standups and the SCRUM artifacts.

- Full Stack Developer
    - Full Stack Developers will be in charge of developing both the backend and the frontend following the requirements for the portion of the function they are in charge of.

- Quality Assurance Tester
    - The Quality Assurance testers are the people in charge of testing the standards of the assigned tasks and functionalities and communicating with the developer for any changes.

Team Member	Role
Kameron	● Project Manager ● Team Leader ● Full Stack Developer ● Quality Assurance Tester
Aiden	● Scrum Master ● Full Stack Developer ● Quality Assurance Tester
Parth	● Full Stack Developer ● Quality Assurance Tester
Jacob	● Full Stack Developer

	• Quality Assurance Tester
An	• Full Stack Developer • Quality Assurance Tester
Khuong	• Full Stack Developer • Quality Assurance Tester

Gantt Chart and Project Roadmap

Gantt Chart

- The Gantt Chart is in a separate file.

Roadmap

- The Roadmap is in a separate file.

Testings

Tests To Do During The Development Phase

1. Unit Test:
    a. A unit test tests all the small testable functions or code within each function during the designing and coding phase.

2. Integration Test:
    a. An integration test tests all the small testable functions or codes working together with other functions or code within each function during the designing and coding phase.

3. End-to-end Test:
    a. An end-to-end test's primary purpose is to test the entire flow of the function after all the component code and functionality work together during the designing and coding phase.

Tests To Do Before The Deployment Phase

4. Usability Test:
    a. A usability test is the process of letting other users, such as the project manager and other group members, test the usability of the functionality before deployment.

5. Regression Test:
    a. A regression test tests any changes within the refracturing stage that will not cause bugs or errors before deployment.

6. Performance Test:
    a. A performance test tests the function endurance under heavier loads using repetition and more amount of users or testers before the deployment phase.

7. Security Test:
    a. A security test tests for errors, bugs, or vulnerabilities within the functionalities before the deployment phase.