**DEPARTMENT OF INFORMATION TECHNOLOGY**

**COURSE CODE: DJ19ITL602 DATE: 03-05-2022**

**COURSE NAME: Software Engineering CLASS: TY B.TECH**

**LAB EXPERIMENT NO. 6A**

**CO/LO:** Analyze real world problems using software engineering principles.

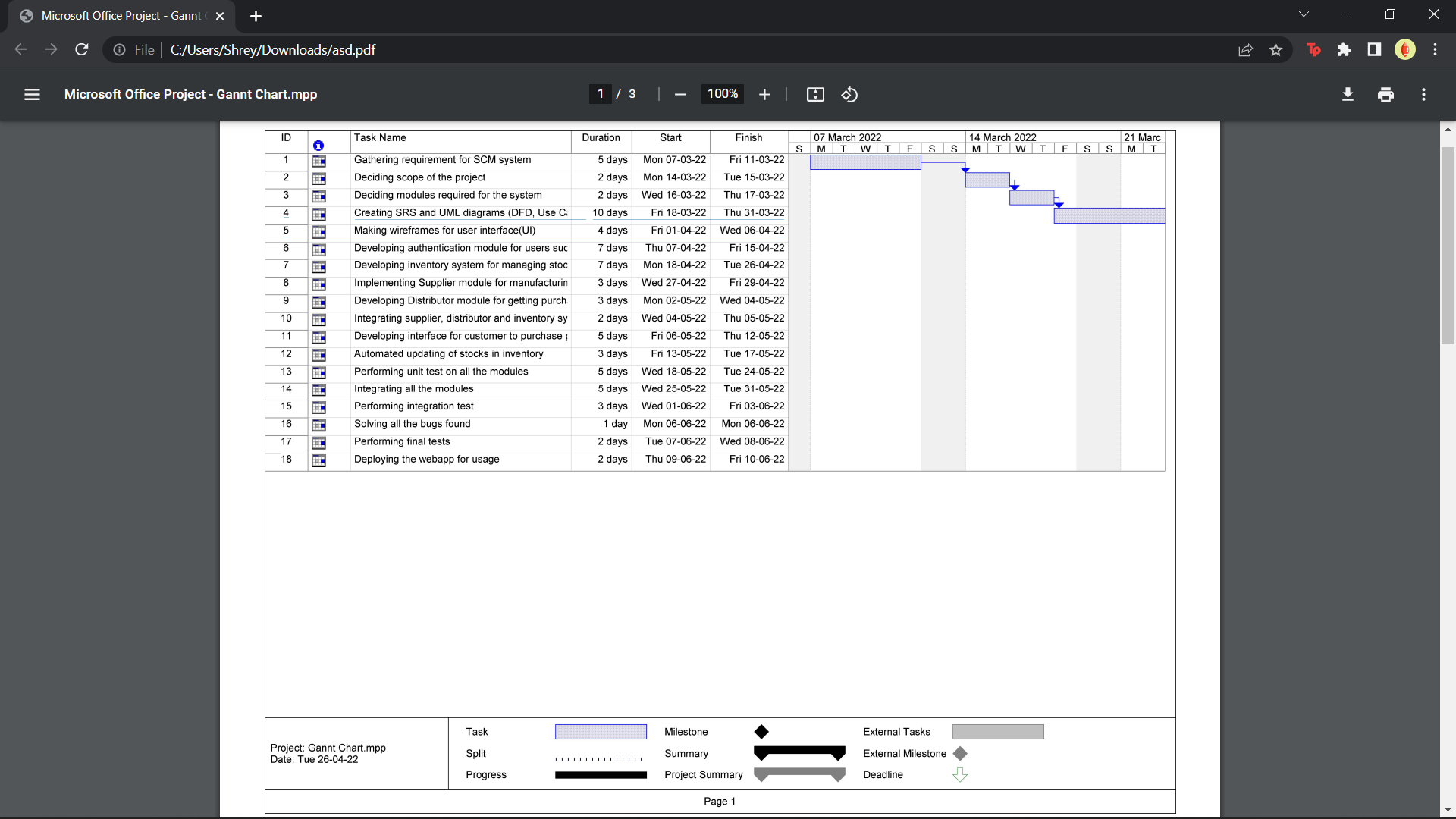
**AIM / OBJECTIVE:** Perform project management activities.

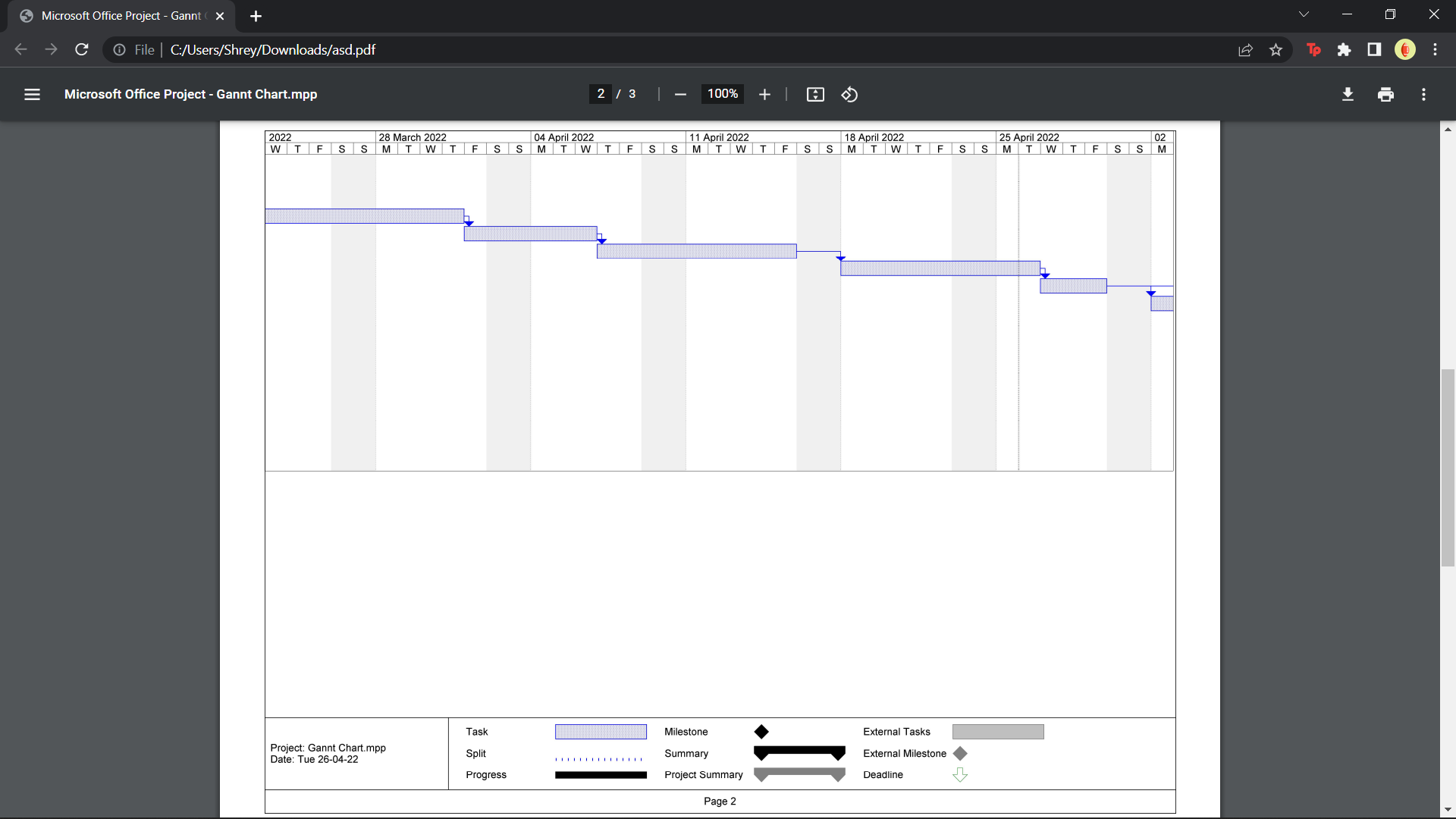
**DESCRIPTION OF EXPERIMENT:**

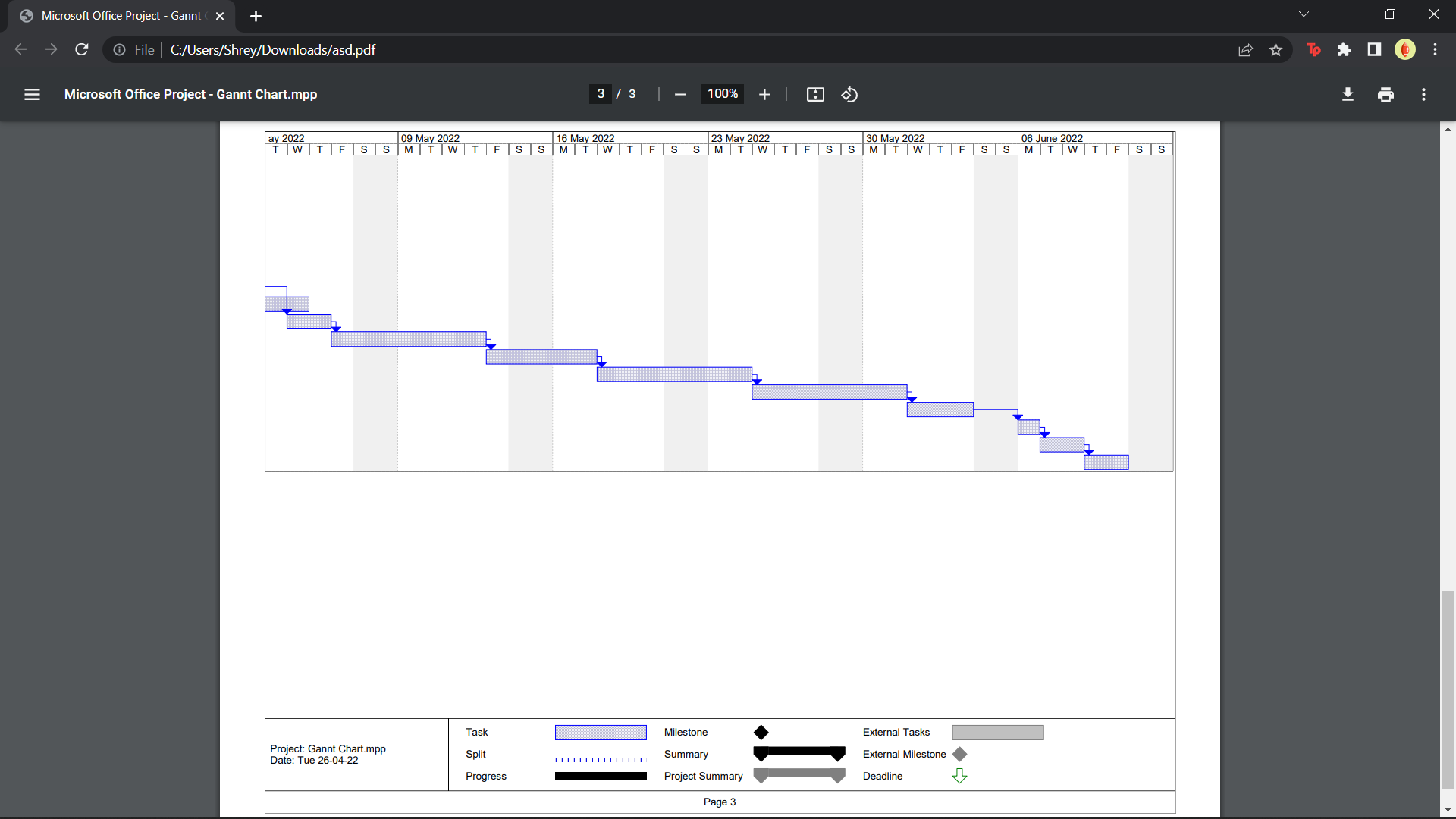
1. Performing Project Scheduling with the help of WBS- Gantt chart
   * Identify the task and sub-tasks to be performed along with their scheduled start and finish dates.
   * Generate Gantt chart using MS project or ready Excel template.
   * Attach and upload the task schedule and generate a Gantt chart.
2. Perform Risk Analysis and design RMMM plan for the system under consideration.
   * identify minimum 5 distinct risks with the system under development.
   * Prepare Risk Information sheet for each risk identified stating the mitigation, monitoring and management activities.
   * Upload minimum 5 Risk Information sheets to complete this objective.

**OUTPUT:**

Gantt Chart:







RMM Plan:

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 1 | Date: 10/5/22 | Prob: 40% | Impact: High |
| **Description:**  Modules might not integrate seamlessly thus causing various errors and inconsistencies in the data. | | | |
| **Refinement/context:**  Due to the huge size of the application, it is divided into many separate independent modules. These modules are developed independently by different development teams and hence there is scope of inconsistencies and incompatibility across the application while integrating. The data might be in different format in different modules increasing the complexity of the overall system integration | | | |
| **Mitigation/ monitoring**   * Prepare well defined structures such as data flow diagrams, er diagrams, sequence diagrams, use case diagrams, class diagrams etc. to provide clarity for the various development teams. * Enable constant communication between development teams to resolve data inconsistency * Ensure integrate each module as soon as it's developed | | | |
| **Management/ contingency plan/ trigger:**   * Try to reverse engineer the errors and fix them as soon as possible. * Develop the most essential features first to provide a basic implementation to the user for use * Hire more engineers to accelerate the process of fixing the bugs and developing respective modules | | | |
| **Current Status**  Mitigation Steps Initiated | | | |
| Originator: Jay | | Assigned: Shrey | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 2 | Date: 10/5/22 | Prob: 80% | Impact : Mild |
| **Description**  Cost of storage of sensitive information might increase miscellaneous costs thus calling for an increase in budget. | | | |
| **Refinement/context**  Since a large amount of data needs to be stored such as supplier details, stock, distributor details etc. Some of the data such as login information also needs to be stored in an encrypted format. All of this combined may lead to huge expenses | | | |
| **Mitigation/ monitoring:**   * Eliminate all non-essential attributes while pre-processing of data * Use commodity hardware to store non-sensitive data * Store data in a distributed format instead of one large data warehouse | | | |
| **Management/ contingency plan/ trigger**   * Additional funds need to be allocated to ensure storage capabilities are met * RAID Storage techniques can be used to improve efficiency of data | | | |
| **Current Status**  Mitigation Steps Initiated | | | |
| Originator: Shrey | | Assigned: Jay | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 3 | Date: 10/5/22 | Prob: 75% | Impact: High |
| **Description**  Only 70% of the components scheduled for reuse will be integrated into the application. The remaining functionality needs to be custom developed. | | | |
| **Refinement/context**  Certain reusable components have been developed by third party applications with no knowledge of design standards. Certain reusable components have been developed that are not supported on the target environment. | | | |
| **Mitigation/ monitoring**   * Contact a third party to determine conformance with design standards. * Check to determine the number of components in and determine if language support can be acquired. | | | |
| **Management/ contingency plan/ trigger**   * Allocate work and funds for developing the respective modules | | | |
| **Current Status**  Mitigation Steps Initiated | | | |
| Originator: Jay | | Assigned: Bhavya | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 4 | Date 10/5/22 | Prob: 70% | Impact: Severe |
| **Description**  Security threat from hackers to steal various database information and sensitive information of the customers such as their information and payment details. | | | |
| **Refinement/context**  Various cybercrimes such as phishing, website hacking and unprotected web services from the hackers that try to steal information and compromise the security of the system are included in this context. These hackers can breach the network to obtain various sensitive information which can make the website unsafe for use. | | | |
| **Mitigation/ monitoring**   * Enforce additional layers of network security. Start from building a firewall. * The third-party web development service provider can provide additional security to the website. * Regular checking for viruses and bugs in the system. * Review potential threats that can be exploited. * A valid certificate for the website should be reviewed on a timely basis and initiation and ending of transactions should be done with SSL certification. | | | |
| **Management/ contingency plan/ trigger**   * The code should be periodically reviewed and any potential threats should be identified and be worked on. As soon as a threat is found immediate action should be taken and the issue should be resolved. * Regular cleaning of the site and unnecessary details should be deleted and the database should be purged of redundant and unnecessary information. | | | |
| **Current Status**  Mitigation steps initiated | | | |
| Originator: Bhavya Patel | | Assigned: Shrey Shah | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 5 | Date: 10/5/22 | Prob: 40% | Impact: Medium |
| **Description**  Making the website compatible with mobile devices, tablets and ipad by making webapps for a better reach and for a better access of the e-commerce website for the users. | | | |
| **Refinement/context**  The website when accessed via mobile and tablet is difficult to access as it has to be opened by a browser which hinders the users to efficiently use the website. The website on tablets and iPad seem to be distorted and the UI/UX should be custom built for such devices. | | | |
| **Mitigation/ monitoring**   * A separate UI/UX should be custom built for the users accessing via mobile devices, iPads and tablets. It should be made easier to use and access. * The changes in the codebase should be made so that it should have parallel computing across different devices. * The database must be strictly monitored to not have inconsistencies during the launch and the making of the webapp for the mobile devices. * The UI must be simple to use and must be according to the device size and should be properly integrated. | | | |
| **Management/ contingency plan/ trigger**   * A separate UI Designer must be hired for the custom development of the webapps. * The database must be backed up and consistent transactions should be updated for the sharing of the database. | | | |
| **Current Status**  Mitigation steps initiated | | | |
| Originator: Shrey | | Assigned: Jay | |

**REFERENCES:**

**​Website References:​**

[1] <https://www.geeksforgeeks.org/risk-mitigation-monitoring-and-management-rmmm-plan/>

[2] <https://en.wikipedia.org/wiki/Gantt_chart>