**Gig Planner Plan – Risk Assessment**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk** | **Likelihood** | **Impact** | **Response** | **Review Actions** | **Reviewed**  **Likelihood** | **Reviewed**  **Impact** |
| Unauthorised people gaining access to database | Medium | High | Set database with restrictions so to limit access by setting password boundary | Database is more secure when password protected.  Use of secret key and database URI  Ensure not visible on github | Medium | Low |
| Not completing tasks on time | Medium | High | Use of Trello board to project manage and have a visual representation of tasks that need to be completed. | Regular use of Trello board and have split tasks into sprints.  Workload and tasks easier to manage.  Clear way to assess current progress. | Low | Low |
| App does not load planer for the user | Medium | High | Use of TDD to ensure that code is working at each stage | Only uploading working code to the master branch | Low | Low |
| Functionality of the app does not work for the user – unable to update or delete | Medium | High | Use of clear unit testing to ensure that the app is working before it is launched to the end user | Using pytest to ensure that all elements of the app are working to produce the desired functionality | Low | Low |
| Users gig planner data is manipulated or stolen | Medium | High | User of user login and password control to ensure authentication and authorisation is correct | At later stage the app will be fitted with a user account and login/password function | Low | High |