EXPERIMENT 4

|  |  |  |  |
| --- | --- | --- | --- |
| RISK INFORMATION SHEET | | | |
| Risk ID: 201 | Date: 12/4/21 | Prob: 40% | Impact: Catastrophic |
| Description:  When data is accidentally deleted, or gets corrupted. Viruses, physical damage or formatting errors can render data unreadable for both humans and software. | | | |
| Refinement/context:  Sub-condition 1: External factors such as viruses transmitted over the web. Subcondition 2: Database hacked.  Sub-condition 3: Unauthorized Access | | | |
| Mitigation/monitoring:  1: Using an antivirus Software.  2: Storing the data using encryption. 3:  Using Strict Access Policy | | | |
| Management/contingency plan/trigger:  Using log-based recovery system to recover the data lost as the data will be stored using log. | | | |
| Current status: 13/4/21: Monitoring Continue | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| RISK INFORMATION SHEET | | | |
| Risk ID: 202 | Date: 13/4/21 | Prob: 50% | Impact: Marginal |
| Description:  Staff might be inexperienced to deal with the complexities of such a corporate project. Resulting in improper management & execution | | | |
| Refinement/context:  Sub-condition 1: Improper Hiring  Sub-condition 2: Employing more freshers than experienced | | | |
| Mitigation/monitoring:  Giving Freshers sufficient training  Using Team/work management software (Trello/Notion/Slack) | | | |
| Management/contingency plan/trigger:  Appointing a person who can manage the staff size and quality | | | |
| Current status: 13/4/21: Monitoring Continue | | | |