|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk No.** | **Risk Name** | **Risk Category** | **Probability** | **Impact** |
| 1. | Software corruption | Technical risk | Low | Negligible |
| 2. | High work load | Business risk | High | Critical |
| 3. | Resource required | Project risk | Low | Negligible |
| 4. | Design and implementation | Project risk | Low | Negligible |
| 5. | Application Complexity | Project risk | High | Critical |
| 6. | Software design | Technical risk | Medium | Marginal |
| 7. | Project size | Project risk | High | Critical |
| 8. | Completion time | Business risk | Very high | Marginal |
| 9. | Hardware failure | Technical risk | High | Critical |
| 10. | Traffic overflow | Business risk | Very high | Catastrophic |
| 11. | Failure in updating profile | Technical Risk | Low | Marginal |
| 12. | No notification of message received | Technical Risk | Low | Critical |
| 13. | Message not sent | Technical Risk | Medium | Critical |
| 14. | Failure to authenticate | Technical Risk | Low | Catastrophic |
| 15. | Database Overflow | Business risk | Medium | Catastrophic |

1. **Risk Table**

Risk Category – 1. Business Risk Impact – 1. Negligible

2. Technical Risk 2. Marginal

3. Project Risk 3. Critical

4. Catastrophic

1. **RMMM Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.: 9** | **Date: 22/03/18** | **Probability:**  High | **Impact:**  Critical |
| **Risk Name:** Hardware failure | | | |
| **Risk Mitigation:**  The cost associated with hardware failure resulting in a loss of data is crucial.  A loss of data will result in not being able to deliver the product to the customer. | | | |
| **Risk Monitoring:**  When working on the product or documentation, the staff member should always be aware of the stability of the computing environment they’re working in. Any changes in the stability of the environment should be recognized and taken seriously. | | | |
| **Risk Management:**  The lack of a stable-computing environment is extremely hazardous to a software development team. In the event that the computing environment is found unstable, the development team should cease work on that system until the environment is made stable again, or should move to a system that is stable and continue working there. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.: 8** | **Date: 22/03/18** | **Probability:**  Very high | **Impact:**  Marginal |
| **Risk Name:** Completion time | | | |
| **Risk Mitigation:**  The cost associated with a late delivery is critical. A late delivery will result in a late delivery of a letter of acceptance from the customer. Without the letter of acceptance, the group will receive a failing grade for the course. Steps have been taken to ensure a timely delivery by gauging the scope of project based on the delivery deadline. | | | |
| **Risk Monitoring:**  A schedule has been established to monitor project status. Falling behind schedule would indicate a potential for late delivery. The schedule will be followed closely during all development stages. | | | |
| **Risk Management:**  Late delivery would be a catastrophic failure in the project development. If the project cannot be delivered on time the development team will not pass the course. If it becomes apparent that the project will not be completed on time, the only course of action available would be to request an extension to the deadline form the customer. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.: 10** | **Date: 22/03/18** | **Probability:**  Very High | **Impact:**  Catastrophic |
| **Risk Name:** Traffic overflow | | | |
| **Risk Mitigation:**  The cost associated with traffic overflow resulting in server crashes is catastrophic.  A server crash will result in the application becoming unresponsive and the service will go down. | | | |
| **Risk Monitoring:**  When working on the application, the developers should always be aware of the scaling of the servers it runs on. Any increase in traffic should be recognized and the servers should scale up to add more resources. | | | |
| **Risk Management:**  The lack of an automated scalable server environment is extremely hazardous to a software application. In the event that the traffic is overflowing, the development team should allocate more servers to the application or migrate it to a more powerful machine. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.: 14** | **Date: 22/03/18** | **Probability:**  Low | **Impact:**  Catastrophic |
| **Risk Name:** Failure to authenticate user | | | |
| **Risk Mitigation:**  Failure to authenticate users into the application can be catastrophic. This can occur due to incorrect or timed out OTP pins that cannot be verified. | | | |
| **Risk Monitoring:**  When creating an authentication workflow in the application, developers must secure OTP codes so that they are correctly sent, and set an appropriate timeout. | | | |
| **Risk Management:**  Failure to authenticate users can cause bad user experience and interrupt their critical tasks. When such an event occurs, users contacting the admins should be responded to and authenticated into the application. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk no.: 15** | **Date: 22/03/18** | **Probability:**  Medium | **Impact:**  Catastrophic |
| **Risk Name:** Database Overflow | | | |
| **Risk Mitigation:**  The cost associated with database overflow resulting in a loss of messages is catastrophic.  An overflow of data in the database will result in new messages not being saved and thus will be lost. | | | |
| **Risk Monitoring:**  When monitoring the deployed application, the developers should always be aware of the status and usage of the database. Any overflow or loss of data in the database should be recognized immediately. | | | |
| **Risk Management:**  The lack of an automated and scalable database systems is extremely hazardous to a software application. In the event that the database overflows, the development team should allocate more database servers to the application or automate the database scaling process based on traffic and usage. | | | |