|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Outcome | Who’s responsible | Risk likelihood | Who it impacts | How to mitigate | Stopping risk |
| DDoS attack | Application is taken offline | Cloud service provider/Developer | Medium | Customer | DDoS protection | Purchase DDoS protection |
| Bugs in application | Application loses users | Developer | Medium | Customer | Constant application testing/ can be used with Jenkins | Tests are performed across all areas of the application to ensure no bugs |
| VM stops working | Loss of data, application taken offline | Cloud service provider | Low | Developer/Customer | N/A – Depends on provider of the VM | Redeploy the VM efficiently to ensure its all working on our end |
| Database VM stops working | Loss of data, protentional breaches | Cloud service provider | Low | Developer/Customer | N/A – Depends on provider of the VM | Redeploy the VM efficiently to ensure its all working on our end |
| Illness to developers | Work on application stops | Developer | Low | Developer/Customer | N/A – must allow for this risk | Ensure all developers see doctors if they feel ill |
| Database gets hacked/leaked | Data leaks, bad publicity | Developer | High | Developer/Customer | Take down the application before any further data leaks happen | Hide the database credentials using environment variables |