|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Description | Date identified | Evaluation | Likelihood | Impact level | Responsibility | Response | Control measures |
| Apps running instance goes down | 25/10/21 | App goes offline | mid | high | Project owner  developers | Rebuild on another computer to get the app back online | Use VSC to quickly recreate machine and store all code in VCS and commits to github |
| App breaking code getting pushed up to main branch | 25/10/21 | App gets broken by faulty code | low | high | Project owner  developer | Git revert back to a stable commit | Double check all code is working before pushing up to main |
| Secrets being upload to github | 25/10/21 | code is exposed and sensitive information could be found by user | mid | high | Developer  Scrum master | Implement a secret key where users cannot access, | use gitignore and secret key before pushing anything to github |
| RDS instance goes down | 25/10/21 | User will not be able to store or retrieve anything on the app | low | high | Developer  Project owner | Make a new RDS instance and connect to it | Testing out the app frequently through the development process |
| Having the correct IAM roles for users | 26/10/21 | Users go over budget because they had access to the wrong role | mid | mid | Project owner  Developers | Use MFA and double check users in group are correct | Monitoring activity on who makes changes in AWS |
| Jenkins VM crashes | 25/10/21 | Test will be unable to automate | low | mid | Developer  Project owner | Have unit testing so can still run tests | Create a new Jenkins vm and build the test again |