|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Description | Assessment | Risk | Impact | Responsibility | Mitigation | Response |
| Downtime from Cloud Service Provider | The services rely on the cloud to keep it running, if in any event it is down it will be | Low | High | Google Cloud Platform | To possibly have a local server which can temporarily negate the effect of the downtime or even another cloud provider overall | Have a fail-safe Jenkins pipeline that will refer to a backup cloud service to avoid a prolonged downtime. |
| Testing of new implementations can break the current build of the project/application | During development changes can bring errors and make the application non functional | Medium | High | Kholeo Taylor | Test everything in development first before pushing to a repository | Set up branches for important individual tasks and review each time until an error occurs which makes it easier to roll back on, leaving the main branches un touched until safe to do so |
| Malicious Attacks | A consideration that an attack can happen such as a DDoS although it may not be likely its still possible to acknowledge | Low | Low | Kholeo Taylor | Having the choice of using a Cloud Service Provider which should have the security to stop any of these attacks from happening | To develop the project in a way it has security features to negate any attack from happening along with utilising what the Cloud Service Provider has to offer |
| Rolling updates downtime | When rolling out a new update to the website/service it can be down for many users during a long period | high | low | Kholeo Taylor | Could block certain features on the application from being utilised until update is completed or notify the user the site will be down momentarily | An orchestration tool can cluster the containers in any event a machine is down, there are others that can take its place in any event that happens negating the downtime |