|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat | Description | Likelihood | Impact | Who’s Responsible | Current Workaround | Proposed Workaround | Response | Tolerance |
| SQL database could be offline if GCP VM is down temporarily. | GCP cannot guarantee 100% service level uptime. While it is very rare to happen, it could be down for maintenance for short periods. | Low | Low | Google Cloud Platform (GCP) | Change application properties in java to point to a h2 database on localhost. As this application only needs to be demonstrated to QA staff. | When taught further into the course, setting up fault tolerance and backup VM’s would automatically point the frontend to the new backup. | Wait for GCP to bring the VM back online. | Tolerate |
| Illness | During the 5 weeks of training for this project, I could become ill (in pandemic times still), impacting my ability to attend every day. | Low | High | Luke Foster | Remain indoors whenever possible, have good levels of hygiene such as washing hands regularly. | None. | None. | Treat, recover as fast as possible. |
| Invalid inputs getting from the frontend all the way to the DB. | The most common mistakes users make on forms are: Leaving fields blank; not ticking at least one box; entering dates in bad formats; entering more characters than allowed in the db field. | High | Medium/high | Luke Foster | Try to catch as many mistakes in front-end logic (JavaScript), and if any get through to the business layer, resolve those too. | None | Code Prompts or alerts into the JS files that alert the user to their mistakes, and only when the form is complete the JSON object sends. | Treat |
| Front-end is HTTP not HTTPS | For this project, the front end will run on a port on the localhost (my machine), this is a regular HTTP page, and not HTTPS which is more secure. | Low | Medium | None | As my application will not contain sensitive information about users, or any sensitive data in general, the low chance of attackers getting access to the information will not hand over damaging data to them. | In future projects the front end can be hosted on platforms that offer the extra security for developers. | Input nothing sensitive into the database or onto the webpage. | Tolerate |

All projects that a company or individual undertakes has associated risks attached to it. The need to analyse these risks from the very start of the project lifecycle is crucial, so that if any of the documented risks are encountered, the workarounds/solutions have already been thought about at least in a satisfactory capacity and can be referenced when needed.

Common risks for online applications are security-based issues, surrounding data transmission and storing it safely. Other risks include users breaking aspects of code through unhandled exceptions, and Cloud Service Provider issues that are out of the developer’s control. Some of these are documented above.