|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the**  **hazard present?**  **Y/N** | **What is the risk?** | Likelihood | Impact | **Risk rating**  **H = High M = Medium**  **L = Low**  M  M | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this in place** | **Action/to do list/outstanding**  **control** |
| Security: risk of database being hacked | Y | Data loss and/or ransom | M | H | H | Strong DB password | Yes | Password could be stronger for production |
| Security: risk of SQL injection | Y | Data loss/unauthorised manipulation | M | H | H | Do not put SQL queries in strings with user input | No | Refactor SQL queries |
| Server could be overloaded with requests | Y | Database could become unavailable | M | M | M | Cloud providers (e.g. GCP) are elastic and adapt to extra load  Monitoring can be implemented to detect extra load and respond  Close database connections when they are not being used | Yes | Monitoring could be implemented |
| Unforeseen bugs in application | Y | Incorrect data could be added to the database; the user experience could be negatively impacted | H | L | M | Thorough debugging and testing, continuous iterative development responding quickly to bug reports | Yes | Better code coverage could be implemented |
| User misuse/abuse of application | Y | Unauthorised manipulation of database, whether intentional or unintentional | M | M | M | Design software robustly in a way that prevents this; provide instructions on how to use the software so that users do not misuse it accidentally | Partly | Design of software could be improved to anticipate misuse; privileged user accounts could be created so that some functions are closed off to most users |

**Com.QA IMS Risk Assessment (List additional hazards, risks and controls particular to your project using this Risk Assessment)**

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible.  **Low Risk (L)** actions should be dealt with as soon as practicable.

**Risk Assessment carried out by: Dan Parkes Date: 13 / 02 / 2020**

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible.  **Low Risk (L)** actions should be dealt with as soon as practicable.

© Alv