|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk | Risk Statement | Response strategy | Objectives | Likelihood | Impact | Risk Level |
| GitHub | Any source code pushed to GitHub could potentially contain information that hackers would find useful when trying to a maliciously alter the project. The source files could potentially contain hard-coded login credentials which could allow for data leaks. | Use stronger passwords and usernames than just “admin” or “root”, and keep them regularly updated. | Reduce the likelihood of hacking and data leaks. | Medium | High | Medium-to-High |
| CoViD-19 | Poses a large risk to the workforce as infection can and will result in major disruption of the workflow. | Enable efficient working from home, ensure workforce is educated on the risks and do not unnecessarily expose themselves. | Reduce the likelihood/ magnitude of infected workforce | Very High | Very high | Very high |
| Lack of necessary technical understanding | Workforce must be educated to the necessary degree in order to execute the tasks at hand effectively. When the technical understanding is not present, this could result in major delays and/or a faulty product. | Ensure the workforce is fully equipped to approach the tasks at hand. | Ensure smooth workflow with minimal disruption, maximise the quality of the resultant product in terms of user experience and security. | Low-Medium | High | Medium |
| Privacy & security | Ensure data is protected where possible/necessary – users may store credentials, payment methods, order details on the system, meaning that careless handling of data may result in severe damages. | Handle data carefully, use encapsulated/private methods, ensure developers have full understanding of responsible data handling processes. | Reduce likelihood of data leaks. | Medium | High | Medium |
| schedule | Ensure a schedule is communicated well between the team and held as closely as possible. Delays may result in an unfinished/untested product being delivered, or delayed. | Use Gantt-charts/Kanban well organised roadmap in order to have clear and good organisation. | Reduce the likelihood of delays. | Low | High | Low |
| Specification miscommunication | There is always a chance of falling to provide a good product, due to a misunderstanding of what the user’s target with the project is. This is particularly true for a problem being developed in a continuous environment. | Ensure clear and frequent communication is upheld between the client and the product owner. | Reduce the likelihood of missing the intention of the client | Low | Medium | Low |
| Incomplete testing | Not all possibilities may have been taken into account when testing using Junit. While SonarQube is a powerful static analysis tool, which is aware of many security hazards, it should not be relied on. | Ensure good understanding of the code’s shortcomings, and address them accordingly. | Reduce the likelihood of security breaches/errors during deployment | Medium | Medium | medium |