IMS Risk Assessment

Risk	Outcome	Responsibility	Impact	Likelihood	Risk factor	Control/mitigation	Response	Impact	Likelihood	Risk factor
Database at risk of being hacked/SQL injection	Loss of data or stolen data	Developers	5	3	15	Strong DB password encrypt traffic so details cannot be intercepted, use third party security like stripe	prevent users from inputing any new information into the database until the issue is resolved, fix the breach, inform relevant authorities	4	2	8
Database servers could be overloaded with requests	Database server could become unstable or even out of commission	Developers	3	3	9	Database could be moved onto a cloud-based server where it can be monitored. If more load is needed the cloud database can be adjusted to match	if the server gets overloaded then it will be migrated over to a cloud-based database. The current database will be monitored	3	1	3
Unforeseen errors or bugs to occur in the application	Connection to the database to break, information not being stored correctly	Developers	3	4	12	High coverage of tests to ensure the code works as it should. quick bug fixes, isolate the bugs so the rest of the application can still work	If we come across bugs, we should aim to resolve them as fast as possible while being thorough to ensure the same bug doesn't occur again	2	3	6

Risk Assessment by: Sean Palla

Date: 26/07/2022