

| Ris | Risk Name              | Date raised  | Risk description  | Likelihood                  | Impact                      | Severity  | Owner                      |
|-----|------------------------|--------------|---|-----------------------------|-----------------------------|---|----------------------------|
| [0] |                        | [dd/mm/yyyy] | [There is a risk that.... If this happens.....]   | [Extreme/High/Moderate/Low] | [Extreme/High/Moderate/Low] | [Extreme/High/Moderate/Low. See Severity Table] | [Person managing the risk] |
| 1   | <b>Schedule Risk</b>   |              |   |                             |                             |   |                            |
|     | Incompletion Risk      | [11/08/2022] | There is a risk that Sprint tasks may not be completed in time.   | Low                         | Extreme                     | High  | Project Team               |
|     | Unavailability Risk    | [02/08/2022] | There is the risk that the various roles external to the group (Project Auditor, Mentor, etc.) are unable to meet at the intended time, potentially delaying the progression of the project (e.g. the delayed release of the Mentor's causing the first mentor meeting to be pushed back a week). | Moderate                    | Moderate                    | Moderate  | External Roles             |
| 2   | <b>Technology Risk</b> |              |   |                             |                             |   |                            |

# Risk Log

|   |                    |              |  |          |          |          |                       |
|---|--------------------|--------------|--|----------|----------|----------|-----------------------|
|   | Obsolence          | [03/08/2022] | As software continues to be updated/modified there's always the possibility that parts of the design solution may soon become obsolete.  | Low      | Moderate | Low      | Project Team          |
|   | Compatibility Risk | [04/08/2022] | At times, we will be working on separate requirements which may require unique/standalone software that hasn't been optimized to be integrated.  | Low      | Moderate | Low      | Project Team          |
| 3 | <b>Client Risk</b> |              |  |          |          |          |                       |
|   | Insufficiency Risk | [09/08/2022] | There is a risk that the Client feels that the requirements established for the design and/or the deliverables provided for the Sprint haven't been sufficiently met.  | Low      | High     | Moderate | Project Team + Client |
|   | Description Risk   | [06/08/2022] | The risk is that the client is unable to appropriately describe or explain the requirement they desire to the project team, leading to a misinterpreted or mismanaged design feature (e.g. Client might suggest a ChatBot with "changing avatars" when they're actually referring to customizable avatars. | Moderate | High     | High     | Project Team + Client |

Risk Log

|   |   |              |  |     |         |          |                       |
|---|---|--------------|--|-----|---------|----------|-----------------------|
|   | Expectation Risk                        | [11/08/2022] | There is the risk that the client firmly requires or expects something of the project team that is potentially out of the course's scope, past the team's ability, or is challenged by time and resource limitations. An example of this would be expecting some fairly complex software such as a face recognition sign-in system as a prioritized requirement.                                   | Low | High    | Moderate | Project Team + Client |
| 4 | Resource Risk                           |              |  |     |         |          |                       |
|   | Resources: Availability & Aecessibility | [04/08/2022] | There is a risk that the project team simply doesn't have access to the resources it needs or that they aren't available at this moment in time. This could be software with an out-of-budget price point (e.g. expensive software implementations), data that requires approval/licensing to use, or software tools that haven't been made available for general use (e.g. non open-source code). | Low | Low     | Low      | Project Team          |
|   | Missing Skill Set Risk                  | [06/08/2022] | There is a possibility that for various reasons the skillset of the team is inadequate/doesn't match the key requirements needed to successfully complete the project. This could be due to factors such as the team underestimating the project when applying, not having the experience or independence to facilitate a group, etc.  | Low | Extreme | High     | Project Team          |
| 5 | Unforseeable Risk                       |              |  |     |         |          |                       |

# Risk Log

|   |                  |              |  |     |          |          |                                 |
|---|------------------|--------------|--|-----|----------|----------|---------------------------------|
|   | COVID-19         | [28/07/2022] | As society continues to adapt to the ongoing presence of COVID-19, a new mutated strain or infecting resurgence is always possible. The potential for delays or shutdowns of in-person meetings or delivery of content remains vulnerable to this and can compromise the completion of the project.    | Low | Moderate | Moderate | Everyone                        |
|   | Member Emergency | [29/07/2022] | There is a possibility that a team member is forced to withdraw from the course or can no longer take part in the project (e.g. health and wellbeing emergency, locational challenges, unit discontinuation, etc.). If insufficiently accounted for, this could have devastating effects on the group. | Low | High     | Moderate | Project Team + Unit Coordinator |
| 6 | IT Risks         |              |  |     |          |          |                                 |
|   | Physical Threats | [12/08/2022] | There is a risk that is brought about by physical threats and vulnerabilities. This could include cyber attacks, damage to IT resources (such as the servers) or even natural disasters, external events, etc.   | Low | High     | High     | Everyone                        |

# Risk Log

|  |                         |              |  |          |      |         |          |
|--|-------------------------|--------------|--|----------|------|---------|----------|
|  | Electronic Threats      | [12/08/2022] | There is a risk of electronic threats, this could be through a security breach, or targeted attack, therefore causing data loss, etc.  | Low      | High | High    | Everyone |
|  | Technical Failures      | [12/08/2022] | There is a risk of Technical failures, if this happens it might cause personal devices to be broken, crash, etc. Therefore it could delay the plan.  | Moderate | High | High    | Everyone |
|  | Infrastructure Failures | [12/08/2022] | There is a risk of infrastructure failure. If this happens, it might cause an Internet disconnect, power outage, etc. Therefore it could interrupt the project.  | Moderate | High | High    | Everyone |
|  | Human Error             | [12/08/2022] | There is a risk of Human error, if this happens it could lead to the accidental deletion of important data, misunderstanding requirements, etc. Therefore it could impact the progress of the project. | High     | High | Extreme | Everyone |

| Mitigating action   | Contingent action   | Progress on actions  | Status                  |
|---|---|--|-------------------------|
| [Actions that can be taken to reduce the likelihood of the risk occurring. May also be acceptance of the risk or transference of the risk e.g. insurance] | [What will be done if this risk does occur. Usually actions to reduce the impact on the project]                                      | [Action taken and date. E.g. <i>Update dd/mm/yyyy mitigation actions implemented</i> ] | [Open, Waiting, Closed] |
|   |   |  |                         |
| Share the schedule and go through upcoming tasks at each weekly meeting.  | Meet immediately, and reschedule tasks if needed.   | Update 11/08/2022<br>mitigation actions implemented                                    | Open                    |
| Schedule comfortably in advance to allow adequate time for changes or clashes.  | Speak to the Unit Co-ordinator if key meetings with external roles aren't able to progress (begins to get detrimental to the project) | Update 12/08/2022<br>mitigation actions implemented                                    | Open                    |
|   |   |  |                         |

## Risk Log

|  |   |   |      |
|--|---|---|------|
| Continuously evaluate the necessary usage of every software and resource used throughout the project. Ask ourselves, "will this technology continue to support the client even after we've concluded"? Discussions with the client and the Team Mentor can help to direct away from resources or technology that may not be sustainable.                                 | Liaise with Client to find the best alternatives to minimise any loss of completion to the Project (considering seeking advice from Mentor)   | Update 11/08/2022<br>mitigation actions implemented | Open |
| Map out the various components of the project and the software/resources that they'll require. Do an initial background check to ensure that there won't be any glaring clashes or conflicts in software used between group members. Ensure that the software is also suitable for the client and will be compatible for their use even after the project has concluded. | Using the Client \$100 priority value ranking, see which requirements are the most critical and resultingly cannot have their software compromised. Software with low/no priority that introduces conflicts can be removed from the project if necessary. | Update 12/08/2022<br>mitigation actions implemented | Open |
|  |   |   |      |
| Regular, well-annotated meetings with the client that continuously account for the changing needs of the client and the abilities/scope of the project team.   | Immediate meeting to mitigate as many of the clients outstanding requirements. Additionally, reflection to ensure it doesn't happen again.  | Update 11/08/2022<br>mitigation actions implemented | Open |
| Regular, well-annotated meetings with the client that continuously account for the changing needs of the client and the abilities/scope of the project team. Additionally, showing the client tangible updates so they're aware of how the product is being developed  | Immediate meeting to mitigate and clearly understand what the client desired and if there's sufficient time/resources to account for that. Additionally, reflection to ensure it doesn't happen again.  | Update 11/08/2022<br>mitigation actions implemented | Open |

|   |  |  |      |
|---|--|--|------|
| A well-done Skills and Resources audit along with a Scope of Work will be helpful in communicating any mismatches in expectations, skillsets, or goals between the Client and Project Team.   | Looks at alternatives or substitutes for the requirement that is more within the scope/abilities of the Project Team (instead of a face recognition system, perhaps a secure PIN login)  | Update 11/08/2022 mitigation actions implemented | Open |
|   |  |  |      |
| A well-done Skills and Resources audit will be fundamental in conveying which resources are desirable, mandatory, and unrequired. From there the Project Team can establish resources it may already have, needs to acquire, or doesn't need to worry about.                              | It will be important to communicate this early on with the Client and look for alternatives or substitutes that will not require the unavailable resource.   | Update 11/08/2022 mitigation actions implemented | Open |
| Thorough research of the project before commencing, a Skills and Resources audit along with a Scope Work should clearly outline what abilities are expected at a base level to successfully complete the project. This will need to be well communicated between the team and the client. | Since this could have a very early detrimental effect on the project, it would require honesty and determination from the Project Team to communicate this with the client and the Unit Coordinator and to discuss a solution. | Update 11/08/2022 mitigation actions implemented | Open |
|   |  |  |      |



# Risk Log

|  |  |   |      |
|--|--|---|------|
| As an unforeseeable risk, there's notably very little that can be done to prevent or mitigate this from happening apart from encouraging vaccination, good hygiene practices, and following expert health advice.                              | In the possibility that this does happen, we are hopefully experienced enough to implement appropriate measures (online communication, remote learning, visual presentation, etc.) | Update 11/08/2022<br>mitigation actions implemented | Open |
| As an unforeseeable risk, there's notably very little that can be done to prevent or mitigate this from happening. Keeping tabs or informed about members' wellbeing or personal situations will keep the team best prepared should it happen. | If this does happen, meet with the Client and Unit Coordinator immediately to discuss how the situation can be handled (reshuffling of tasks/timelines, requirements leniency)     | Update 11/08/2022<br>mitigation actions implemented | Open |
|  |  |   |      |
| As our project on Github is private, it can effectively reduce the threat of outsiders.  | Document and analyze the situation to update, change or improve procedures   | Update 12/08/2022<br>mitigation actions implemented | Open |

## Risk Log

|  |   |  |      |
|--|---|--|------|
| As our project is non-profit and non-commercial, it can reduce the chance of this problem and as always we should make a backup of our work. | If this risk does occur, it's essential to have a backup and clearly state the situation to the mentor, client and auditor.   | Update 12/08/2022<br>mitigation actions<br>implemented | Open |
| Regularly check personal devices, store important files in mailboxes, one drive, etc.  | Explain the situation to the team and postpone or change the plan.  | Update 12/08/2022<br>mitigation actions<br>implemented | Open |
| Pay attention to the announcement and report the situation to the team in time.  | If it is too late to explain the situation in advance, supplementary explanations are required afterward, and specific situations require specific handling.  | Update 12/08/2022<br>mitigation actions<br>implemented | Open |
| Always make a backup of the work, and report the situation to the team in time.  | Control the incident and prevent further damage to the project. Find out the cause of the incident and remove the affected file or program, then recover these files and programs after eliminating the threat. | Update 12/08/2022<br>mitigation actions<br>implemented | Open |