# Inception Phase Status Assessment

## 1. Assessment against Objectives of the Inception Phase

### 1.1 Do we know what we are trying to achieve?

The aim of the project is to develop a resource planning tool this is embodied in the completed Vision Document.

We understand the main functional requirements of the project which are:

Authenticate with system

Update skills

Remove skills

Create project

Update project

Locate resource

View user allocation

View unassigned resources

Add system users

Remove user

View upcoming projects

Request to join project

Add resource requirement to project

Update resource requirement

Remove resource requirement

Notify of new project assignment

Notify of resource double booking

View organisational requirements

This is shown in the completed Functional Requirement model embodied in Requirements document, short use case description, domain model and the use case diagram

We understand the main Non-Functional requirements of the project which are:

The product keeps the information secure

The Application is efficient and easy to use

The application can handle the complete team using it if required

The application is responsive

This is shown in the completed Non-Functional Requirement model embodied in the Non Functional requirements specification document

### 1.2 Do we know how we are going to achieve it?

We have a good idea of how we are going to achieve our aims. We are going to use a web application which stores data in a database, using various persistence frameworks. This is shown in the completed Architecture notebook

We have a good understanding of the project specific risks facing our project and how we are going to deal with them. The risks are:

Appropriately securing information

Sponsor maintains support

The team’s skillset is adequate enough

Scope creep / Under scoped

Our evolving understanding of risks is shown in the ongoing risk list and discussed further below in Section 4.

We have a good understanding of how we are going to check that our application delivers the intended functionality and system properties. Our key areas of concern and the test strategies we will use to address these concerns are as follows:

Functional testing

Unit testing

Integration Testing

User acceptance testing

This is shown in the completed Master Test Plan

We have a good understanding of the dependencies and likely completion times for different parts of the project. Target completion dates for key aspects of the project are as follows:

*Architecture:*

***13/05/2019***Implement 1st & 2nd highest priority to support CCRD use case

***27/05/2019***Implement 3rd highest priority to support CCRD use case

*Functionality:*

***12/08/2019***Top 3 CCRD use cases to be implemented

*Testing:*

***29/07/2019***Complete development and integration testing for 2nd highest priority use case(s)

***12/08/2019***Complete development and integration testing for 3th highest priority use case(s)

***26/08/2019***Complete development and integration testing for 4th highest priority use case(s)

*Documentation:*

***26/08/2019***Complete user documentation - how to use the system for each user, admin documentation that explains how to configure and setup system.

This is shown in the Initial Project Plan.

### 1.3 Skills required

Our project requires skills using the following key tools and technologies:

MySQL

Java

Maven

Git

Tomcat

SpringBoot

JPA

Hibernate

JavaScript

HTML

CSS

We have demonstrated that we have the skills to use these technologies through the implementation of a technology competency demonstrator.

**2. Deliverables**

### 2.1 *Project vision*

This document contains only a rough outline of the intended application; there were no issues in producing the document

### 2.2 *Initial requirement model*

This document is important as it outlines what we need to produce for the completion of the project. There were issues with initial scoping of uses cases for this document

### *2.3 Proposed architecture*

This document consists of how we will combine all required components together: No issue.

### *2.4 Risk List*

The risk list is a document that can never be completed until the project is finished, as new risks and issues can arise at any time. This document is well written and contains key components which the team must look out for. There were no issues in producing this document

### *2.5 Master test plan*

No issues

### *2.6 Initial project plan*

No issues

### *2.7 Technical competency demonstrator*

Matt got stuck for a long time on the Technical Competency demonstrator, mainly SpringWebMVC. He was sending back an integer ID form a form and asking the system to treat that as an Object that needs to be looked up by ID. He nearly gave up and wanted to switch technologies but﻿﻿﻿﻿﻿﻿﻿﻿﻿ worked out how to use a Converter correctly. He started using Spring but switched to SpringBoot for automatic configuration, it didn’t solve the original problem and wasn't necessary but he kept it anyway as embedded Tomcat and database proved to really simplify setup. He couldn't get Hibernate working correctly, but worked out he needed to use JPA as well, as Hibernate is a specific implementation of JPA. In the end he was happy that each of the technologies would work and would meet requirements. The demonstrator performs a few simple CRUD operations to make use of each of the technologies.

## 3. General Issues

## No issues

## 4. Risks

### 4.1 *system incompatible with sponsors systems*

If the system cannot be used by the sponsor then the system is not able to be used by the sponsor.

The key mitigation strategy is to develop a program which is compatible with most systems.

### *4.2 Poor use of version control*

This risk can cause project delays if the team does not appropriately use version control which will cause the project to fail.

The mitigation strategy is to use a common version control system with available help online.

This risk is resolved.

### *4.3 Team has inadequate skill set*

This risk can cause the project delays in the form of team members only learning requisite technologies when they need them which can make developing the application take longer than required.

The mitigation strategy for this is to use skills taught during the CSU Computer science bachelors and to occasionally have skill quizzes to ensure the teams skills are up to date.

This risk is still open but being managed

### *4.4 Team members leave the project*

Team members leave the project, due to the small project team some use cases will have to be removed.

The mitigation strategy is to ensure that team members are all well communicated to and for the team to be open with each other to manage expectations.

This risk is still open and being managed

### *4.5 Inadequate security*

If the program is not secure enough to store data then the users will not use it.

Will ensure security of the data is appropriate to the requirements.

This risk is still open and being managed

### *4.6 Incapable of providing needed functionality*

The risk of not meeting the client’s needs can lead to refusal of product purchase thus a waste of time and money on part of the developer’s alongside a potential loss of reputation.

The mitigation strategy is to establish the project requirements and selecting technologies that can deliver the services required by the client.

This risk is resolved.

### *4.7 Team unable to identify or procure technologies*

*If team members are unable to determine the technologies that should be used, the project will cease to proceed past the planning phase.*

*The mitigation strategy is to investigate early into the technologies to be used.*

*This risk is resolved.*

## 5 Summary – Overall Project Progress

The project status is Green, we have completed each of the aims of the Inception Phase.

We did have an ongoing issue with Jack’s version control, Matt resolved over TeamViewer.

We have not investigated security yet. There is some concern of ongoing risk in implementing secure authentication. We will need to do some research of how we host the solution, and if we can get a TLS certificate for testing over HTTPS.

We have not reviewed Brodie’s quiz, cannot assess ongoing risk of insufficient skills.